

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

DARRYL SMALL, individually and on behalf  
of all others similarly situated,

Plaintiff,

vs.

MULTICARE HEALTH SYSTEM D/B/A  
MULTICARE,

Defendant.

Case No. 3:24-cv-05552

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Darryl Small, a patient of MultiCare Health System d/b/a MultiCare (“MultiCare” or “Defendant”), brings this class action lawsuit against Defendant individually and on behalf of all others similarly situated and alleges, upon personal knowledge as to his own actions and his counsel’s investigation and—where indicated—upon information and good faith belief as to all other matters, as follows:

**I. INTRODUCTION**

1. Plaintiff brings this action individually and on behalf of millions of other patients (collectively, the “Users”) whose medical privacy was violated by MultiCare’s use of

1 tracking and data collection tools by Alphabet, Inc. d/b/a Google (“Google”) and Meta  
2 Platforms, Inc. d/b/a Meta (“Meta” or “Facebook”).<sup>1</sup>

3 2. Plaintiff, a MultiCare patient, alleges that Defendant installed Google and Meta  
4 Collection Tools on their public website (<https://www.multicare.org/>, the “Website”) and their  
5 patient portal (available at <https://www.multicare.org/patient-resources/mychart/>, “Patient  
6 Portal”) (collectively, the “Web Properties”) to simultaneously collect and divulge Users’  
7 confidential health information (“Private Information” including personally identifiable  
8 information (“PII”) and protected health information (“PHI”)) to Google and Meta in  
9 violation of federal and state laws.

10 3. MultiCare used Google Collection Tools and Meta Collection Tools to divulge  
11 the Private Information of Users of its Web Properties for marketing, re-marketing and  
12 analytics purposes despite its express promise that: “All other information that is shared in a  
13 way not addressed in this notice, including uses or disclosures for marketing purposes, or  
14 disclosures of your information in exchange for some form of payment, will be made **only**  
15 ***after you give your written permission*** or as required by law.”<sup>2</sup>

16 4. The Private Information of potentially millions of Users of MultiCare’s Web  
17 Properties was improperly and unlawfully disclosed to Google and Facebook without their  
18 knowledge or consent. MultiCare did so because it knew that this sensitive information had  
19 tremendous value and that Plaintiff and Class Members would **not** consent to the collection,  
20 disclosure and use of their Private Information if they were provided a choice or would  
21 demand significant compensation.

22  
23  
24 <sup>1</sup> The Facebook tracking and data collection tools include the Meta Pixel, Meta SDK, Meta Conversions API,  
25 customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions and similar collection  
26 tools (collectively, “Meta Collection Tools”). The Google tracking and collection tools include Google Analytics,  
27 Google Tag Manager, DoubleClick, social plug-ins, server-to-server transmissions and similar collection tools  
(collectively, “Google Collection Tools”).

<sup>2</sup> See <https://www.multicare.org/about/policies-notices/website-privacy-policy/> (last visited June 28, 2024)  
(emphasis added).

1           5.     MultiCare encouraged and/or required Plaintiff and Class Members to use its  
2     Web Properties, including its Patient Portal, to receive healthcare services, and MultiCare’s  
3     Web Properties encourage and require Users to provide Private Information in order to  
4     facilitate healthcare treatment including, but not limited to, to search for a doctor, learn more  
5     about their conditions and treatments, access medical records and test results and manage  
6     appointments.

7           6.     At all times that Plaintiff and Class Members visited and utilized MultiCare’s  
8     Website and Patient Portal to receive medical services, they had a reasonable expectation of  
9     privacy that their Private Information would remain secure and protected and only utilized for  
10    medical purposes.

11          7.     Further, MultiCare made express and implied promises to protect Plaintiff’s and  
12    Class Members’ Private Information and maintain the privacy and confidentiality of  
13    communications that patients exchange with MultiCare.

14          8.     Simply put, MultiCare broke those promises again and again.

15          9.     The Facebook tracking pixel (the “Meta Pixel”)—installed and configured by  
16    MultiCare—is a “piece of code” that allowed MultiCare to “measure the effectiveness of [its]  
17    advertising by understanding the actions [Users] take on [its] site.”<sup>3</sup> It also allowed MultiCare  
18    to optimize the delivery of ads, measure cross-device conversions, create custom advertising  
19    groups or “audiences,” learn about the use of the Web Properties and optimize advertising and  
20    marketing costs.<sup>4</sup>

21          10.    The Google Collection Tools, installed and configured by MultiCare, operate  
22    similarly to the Meta Pixel and other Meta Collection Tools.

---

26    <sup>3</sup> <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Jun. 19, 2024).

27    <sup>4</sup> *Id.*

11. Invisible to the naked eye, pixels—which are configured by the website owners, here, MultiCare—collect and transmit information from Users’ browsers to unauthorized third parties including, but not limited to, Google and Meta.<sup>5</sup>

12. In particular, the Meta Pixel tracks visitors to the Web Properties and the actions they take as they interact with the website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).<sup>6</sup>

13. MultiCare purposively and intentionally installed the Google and Meta Collection Tools on its Web Properties and configured the Google and Meta Collection Tools to transmit and disclose Plaintiff’s and Class Members’ Private Information to Facebook.

14. Operating as designed, MultiCare’s Google and Meta Collection Tools allowed the Private Information that Plaintiff and Class Members submitted to MultiCare to be unlawfully disclosed to Facebook.

15. For example, when a User uses MultiCare’s Web Properties, the Meta Pixel and/or Google Analytics directed Plaintiff’s or Class Members’ browser to send a message to Facebook’s/Google’s servers, those messages transmitted the content of their communications to Meta/Google, including, but not limited to: (1) signing-up for the Patient Portal; (2) signing-in to the Patient Portal; (3) requesting copies of medical records; (4) paying medical bills; (5) making, scheduling, or participating in appointments; (6) exchanging communications relating to doctors, treatments, payment information, health insurance

---

<sup>5</sup> The Google and Meta Collection Tools include small snippets of code placed on webpages by the website owner, for example, pixels or tags. The process of adding the Google and Meta trackers to a webpage is a multi-step process that must be undertaken by the website owner, here, MultiCare.

<sup>6</sup> A pixel is a piece of code that “tracks the people and type of actions they take.” RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Jun. 19, 2024). Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, MultiCare utilized the data collected by the Google and Meta Collection Tools, including pixels and tags, to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

1 information, prescription drugs, prescription side effects, conditions, diagnoses, prognoses, or  
2 symptoms of health conditions; (7) conduct a search on MultiCare's Web Properties and (8)  
3 other information that qualifies as PHI under federal and state laws.

4 16. The transmission of Plaintiff's PHI as described above occurs simultaneously  
5 from Defendant's Web Properties to both Google and Meta.

6 17. The information transmitted from MultiCare's Web Properties to Google and  
7 Meta includes information sufficient to identify a specific patient under federal law (such as  
8 IP address information, device identifiers, advertising identifiers that Meta associates with a  
9 patient's Facebook account and identifiers that Google associates with a patient's identity—  
10 including a unique cookie ID and/or their IP address)—and may also include a patient's  
11 demographic information, email address, phone number, computer ID address or contact  
12 information entered as emergency contacts or for advanced care planning, along with  
13 information like appointment type and date, a selected physician, button and menu selections,  
14 the content of buttons clicked and typed into text boxes, and information about the substance,  
15 purport, and meaning of patient requests for information from MultiCare under federal and  
16 state health privacy laws.

17 18. Among the personally identifying information that MultiCare disclosed is the  
18 User's unique and persistent Facebook ID which allows Facebook and other third parties to  
19 personally identify that User and associates the Users' Private Information with its Facebook  
20 profile. The Facebook ID is a string of numbers Facebook uses to identify and connect to a  
21 User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you  
22 choose to create a username.<sup>7</sup> Thus Facebook, which creates and maintains the Facebook ID  
23 directly connected to a User's Facebook account, utilizes the Facebook ID to personally  
24 identify each User whose Private Information is disclosed to it.

25  
26  
27 <sup>7</sup> See <https://www.facebook.com/help/211813265517027> (last visited Jun. 19, 2024).

1           19. Transmitting the Private Information allows a third party (*e.g.*, Google and/or  
2 Meta/Facebook) to know that a specific patient was seeking confidential medical care. This  
3 type of disclosure could also allow a third party to reasonably infer that a specific patient was  
4 being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

5           20. Google collects the transmitted identifiable health information and uses cookies,  
6 IP addresses, and other unique identifiers to match it to Google users, allowing MultiCare to  
7 target advertisements both on and off Google. For example, MultiCare and Google can target  
8 ads to a person who has used the Website or the Patient Portal and exchanged  
9 communications about a specific condition, such as cancer.

10           21. Similarly, Meta collects the transmitted identifiable health information and uses  
11 cookies, IP addresses, and other unique identifiers to match it to Facebook users allowing  
12 MultiCare to target advertisements both on and off Facebook. For example, MultiCare and  
13 Meta can target ads to a person who has used the Website or the Patient Portal and exchanged  
14 communications about a specific condition, such as cancer.

15           22. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”),  
16 Pub. L. No. 104-191, 110 Stat. 1936 (1996), and state analogs prohibit healthcare providers  
17 from sharing health care information, medical records and related information with third  
18 parties except as needed for a patient’s treatment, payment or with their consent.

19           23. Importantly, these laws give patients a reasonable expectation of privacy in  
20 communications with healthcare providers relating to their medical conditions and treatment,  
21 because this information may not be disclosed outside the healthcare setting without notice  
22 and consent.

23           24. The Office for Civil Rights (“OCR”) at the United States Department of Health  
24 and Human Services (“HHS”) recently re-affirmed that HIPAA and its regulations prohibit  
25 the transmittal of individually identifiable health information (“IIHI”) by tracking technology  
26  
27

1 like the Meta Pixel without the patient’s authorization and other protections like a business  
2 associate agreement with the recipient of patient data.<sup>8</sup>

3 25. Reiterating the importance of and necessity for data security and privacy  
4 concerning health information, the Federal Trade Commission (“FTC”) recently published a  
5 bulletin entitled *Protecting the privacy of health information: A Baker’s dozen takeaways*  
6 *from FTC cases*, in which it noted that:

7 [h]ealth information is not just about medications, procedures, and  
8 diagnoses. ***Rather, it is anything that conveys information—or***  
9 ***enables an inference—about a consumer’s health.*** Indeed,  
10 [recent FTC enforcement actions involving] *Premom*, *BetterHelp*,  
11 *GoodRx* and *Flo Health* ***make clear that the fact that a consumer***  
12 ***is using a particular health-related app or website—one related***  
13 ***to mental health or fertility, for example—or how they interact***  
14 ***with that app (say, turning ‘pregnancy mode’ on or off) may***  
15 ***itself be health information.***<sup>9</sup>

16 <sup>8</sup> See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,  
17 <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (noting that “IIHI  
18 collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an  
19 existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or  
20 geographic location, does not include specific treatment or billing information like dates and types of health care  
21 services.”). This guidance was recently vacated *in part* by a federal district court in the Northern District of Texas  
22 due to the court finding it in part to be the product of improper rulemaking, and it is cited for reference only until  
23 the OCR updates its guidance, should it do so in the future. See *American Hosp. Ass’n. v. Becerra*, 2024 WL  
24 3075865 (S.D. Tex., Jun. 20, 2024). Notably, the Court’s Order found only that the OCR’s guidance regarding  
25 covered entities collection and disclosure to third parties of users’ IP addresses while they navigated *unauthenticated*  
26 *public webpages* (“UPWs”) was improper rulemaking. The Order in no way affects or undermines the OCR’s  
27 guidance regarding covered entities disclosing unique personal identifiers, such as Google or Facebook identifiers,  
to third parties while patients were making appointments for particular conditions, paying medical bills or logging  
into (or using) a patient portal. See *id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the “Proscribed  
Combination” defined as “circumstances where an online technology connects (1) an individual’s IP address with  
(2) a visit to a UPW addressing specific health conditions or healthcare providers” but stating that “[s]uch vacatur  
is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane  
HHS document.”). Furthermore, the Federal Trade Commission’s (“FTC”) bulletin on the same topics remains  
untouched as do the FTC’s enforcement actions against numerous healthcare providers for using similar (if not  
identical) collection tools as MultiCare.

<sup>9</sup> See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the  
FTC Business Blog (July 25, 2023) (emphasis added), available at [https://www.ftc.gov/business-](https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases)  
guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Apr.  
19, 2024).

26. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

**Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**

In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***

[Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.***<sup>10</sup>

27. Not only did MultiCare willfully and intentionally incorporate the Google and Meta Collection Tools into its Web Properties, but it also never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Web Properties with Google or Facebook.

28. As a result, Plaintiff and Class Members were unaware that their PII and/or PHI were being surreptitiously transmitted to Facebook and Google as they communicated with their healthcare providers, looked up their conditions and/or treatments, and logged into the Patient Portal.<sup>11</sup>

<sup>10</sup> *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

<sup>11</sup> In contrast to MultiCare, several healthcare providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g., Cerebral, Inc. Notice of HIPAA Privacy Breach*, [https://cerebral.com/static/hippa\\_privacy\\_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf](https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf) (last visited Apr. 19, 2024); Annie Burky, *Advocate Aurora says 3M*



29. The full extent of MultiCare’s unlawful disclosures is not yet known, but the numbers may be staggering. According to MultiCare’s Website, they employ “our comprehensive system of health includes more than 300 primary, urgent, pediatric and specialty care locations across Washington, Idaho and Oregon, as well as 12 hospitals. We welcome patients from the entire Pacific Northwest region and our 20,000-plus team members — including employees, providers and volunteers — proudly care for the communities we serve.”<sup>12</sup>

30. MultiCare owed common law, contractual, statutory and regulatory duties to keep Users’ communications and medical information safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from Users’ Private Information, MultiCare assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

31. MultiCare, however, failed in its obligations and promises by utilizing Google and Meta Collection Tools on the Web Properties, such as Google Analytics and the Meta Pixel, knowing that such technology would transmit and share Plaintiff’s and Class Members’ Private Information with unauthorized third parties.

32. MultiCare breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure its Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users’ information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their Private Information to Google, Facebook, or others; (iv) failing to take steps to block the transmission of Plaintiff’s and Class Members’ Private

---

*patients’ health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3> (last visited Jun. 19, 2024); *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (August 17, 2022), [\(https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-pixel#:~:text=August%2017%2C%202022%20%2D%20North%20Carolina,protected%20health%20information%20\(PHI\)\)](https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-pixel#:~:text=August%2017%2C%202022%20%2D%20North%20Carolina,protected%20health%20information%20(PHI)) (last visited Jun. 19, 2024).

<sup>12</sup> See <https://www.multicare.org/about/> (last accessed June 28, 2024).

Information through the Google and Meta Collection Tools or any other tracking technologies; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Web Properties in order to maintain the confidentiality and integrity of patient Private Information.

33. MultiCare's interception, dissemination and use of Private Information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties.<sup>13</sup>

34. MultiCare has also been unjustly enriched by its misconduct, obtaining unearned revenues derived from the enhanced advertising services and more cost-efficient marketing on Facebook and Google it receives in exchange for its unauthorized disclosure of patient information.

35. Plaintiff seeks to remedy these harms individually and for millions of similarly affected persons, and therefore brings causes of action for (i) Violations of the Electronic Communications Privacy Act 18 U.S.C. § 2511(1), *et seq.*; (ii) Breach of Express Contract; (iii) Breach of Implied Duty of Good Faith and Fair Dealing; (iv) Breach of Implied Contract; (v) Negligence; (vi) Breach of Fiduciary Duty; (vii) Unjust Enrichment; (viii) Invasion of Privacy and (ix) Violations of the Washington Consumer Protection Act, Wash. Rev. Code. Ann. §§ 19.86.020, *et seq.*

## II. PARTIES

36. Plaintiff Darryl Small is a natural person and a citizen and resident of Michigan. Prior to July 2024, and throughout the class period, Plaintiff was a citizen and resident of Kitsap County in Washington.

---

<sup>13</sup> It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (*e.g.*, Twitter, Bing, LinkedIn, HotJar, LifePerson, CrazyEgg, BlueKai, Bidtellect, Yahoo, The Trade Desk, Adobe or others) for the purposes of building or enhancing profiles and retargeting or to insurance companies to set rates, among other things.

37. Defendant MultiCare Health System d/b/a MultiCare is a Washington nonprofit corporation with its principal place of business at 820 A St., Tacoma, WA, 98402-5202. Defendant is a large health care delivery system with “Nine acute-care adult hospitals in Auburn, Covington, Olympia, Puyallup, Tacoma, Spokane, Spokane Valley and Yakima; Two behavioral health hospitals in West Seattle and Tacoma; One acute-care pediatric hospital in Tacoma that is the regional referral center for southwest Washington; More than 290 primary care, specialty care and urgent care clinics in Pierce, King, Kitsap, Thurston, Snohomish, Spokane and Yakima counties; Five neighborhood emergency departments; More than 2,000 MultiCare staff providers; [and] More than 22,000 employees.”<sup>14</sup>

38. Headquartered in Tacoma, MultiCare is one of the largest health systems in the state of Washington. MultiCare advertises its 2023 total patient volume on its website: “Emergency Department visits: 644,651; Inpatient surgeries: 20,788; Outpatient surgeries: 58,801; Admissions: 100,589; Births: 11,841; Home health admits: 3,400; Hospice admits: 2,189.”<sup>15</sup>

39. MultiCare is a covered entity under HIPAA.

### III. JURISDICTION & VENUE

40. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, including the Electronic Communications Privacy Act (“ECPA”), 28 U.S.C. § 2511, *et seq.*

41. The Court has supplemental jurisdiction over Plaintiff’s claims arising under state law under 28 U.S.C. § 1367.

42. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than one hundred members in the

<sup>14</sup> See <https://www.multicare.org/newsroom/multicare-facts/> (last accessed June 28, 2024).

<sup>15</sup> *Id.*

1 proposed Class, and at least one member of the class is a citizen of a state different from  
2 MultiCare.

3 43. This Court has personal jurisdiction over Defendant because its principal place  
4 of business is in this District and a substantial portion of the acts and omissions giving rise to  
5 Plaintiff's claims occurred in and emanated from this District.

6 44. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant  
7 resides in this district and a substantial part of the events and omissions giving rise to  
8 Plaintiff's claims occurred in this district.

#### 9 **IV. FACTUAL BACKGROUND**

##### 10 **A. MultiCare Secretly Disclosed & Permitted Third Parties to Intercept Plaintiff's &** 11 **Class Members' PHI.**

12 45. MultiCare maintains and operates the Web Properties, by and through which it  
13 encouraged and/or required patients to seek healthcare services.

14 46. To obtain healthcare services through the Web Properties, Plaintiff and other  
15 Class Members were required to provide their PHI and/or PII to MultiCare.

16 47. Each step of this process was tracked and logged by the Google and Meta  
17 Collection Tools.

18 48. On information and good faith belief, throughout the Class Period, the process  
19 for obtaining healthcare services on the Web Properties has been substantially the same in all  
20 material respects throughout the United States.

21 49. Completely unbeknownst to Plaintiff and other Class Members, beginning as  
22 early as approximately May 2008 and continuing through present, Private Information that  
23 they communicated to MultiCare through the Web Properties while obtaining healthcare  
24 services was disclosed to Google.

25 50. Completely unbeknownst to Plaintiff and other Class Members, from  
26 approximately December 2014 to at least November 2020, Private Information that they  
27

communicated to MultiCare through the Website while obtaining healthcare services was disclosed to Meta.

**1. MultiCare Improperly Disclosed Plaintiff's & Class Members' Private Information to Meta.**

51. MultiCare utilized Facebook advertisements and intentionally installed the Meta Pixel on its Web Properties.

52. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare Partners. Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

53. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.<sup>16</sup>

54. Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta healthcare Partner's website embedded with the Meta Pixel, the Meta Pixel will be triggered to send Meta "Event" data that Meta matches to its Users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Meta Pixel can then be used to measure the effectiveness of an advertising campaign.<sup>17</sup>

<sup>16</sup> Meta Business Help Center, *About Customer List Custom Audiences* (2023), <https://www.facebook.com/business/help/341425252616329?id=2469097953376494>.

<sup>17</sup> Meta Business Help Center, *About Customer List Custom Audiences* (2023), <https://www.facebook.com/business/help/341425252616329?id=2469097953376494>; see also, Meta Blueprint, *Connect your data with the Meta Pixel and Conversion API* (2023), [https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d\\_fnzRCUAhKGYsLqNA-VcLTMr3G\\_hxxFr3GZC\\_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa](https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa)

1           55. Meta also allows Meta healthcare Partners to create a Custom Audience by  
2 uploading a patient list to Meta. As Meta describes it:<sup>18</sup>

3 A Custom Audience made from a customer list is a type of audience you can create to  
4 connect with people who have already shown an interest in your business or product. It's  
5 made of information - called "identifiers" - you've collected about your customers (such as  
6 email, phone number and address) and provided to Meta. Prior to use, Meta hashes this  
information.

7 Then, we use a process called matching to match the hashed information with Meta  
8 technologies profiles so that you can advertise to your customers on Facebook, Instagram  
9 and Meta Audience Network. The more information you can provide, the better the match  
10 rate (which means our ability to make the matches). Meta doesn't learn any new identifying  
information about your customers.

11           56. Meta provides detailed instructions for healthcare Partners to send their  
12 patients' individually identifiable information to Meta through the customer list upload. For  
13 example:

14 **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you  
15 provide us with information about your existing customers and we match this information  
16 with Meta profiles. The information on a customer list is known as an "identifier" (such as  
email, phone number, address) and we use it to help you find the audiences you want your ads  
to reach.

17 Your customer list can either be a CSV or TXT file that includes these identifiers. To get the  
18 best match rates, use as many identifiers as possible while following our formatting  
19 guidelines. You can hover over the identifiers to display the formatting rules and the correct  
column header. For example, **first name** would appear as **fn** as a column header in your list.

20 Alternatively, we have a file template you can download to help our system map to your  
21 identifiers more easily. (You can upload from Mailchimp as well.)

22           57. Meta healthcare Partners can then use the Custom Audiences derived from their  
23 patient list with the Meta Pixel and Pixel Events for Meta marketing campaigns and to  
24 measure the success of those campaigns.

25  
26 <sup>18</sup> Meta Business Help Center, *About Customer List Custom Audiences* (2023),  
27 <https://www.facebook.com/business/help/341425252616329?id=2469097953376494>.

1           58. Without discovery, Plaintiff does not yet know whether MultiCare uploaded  
 2 patient lists to Meta. However, Plaintiff does know that when they and Class Members sought  
 3 and used MultiCare's Web Properties, their Private Information was intercepted concurrently  
 4 in real time and then disseminated to Facebook and potentially to other third parties, via the  
 5 Meta Pixel and other Meta Collection Tools that MultiCare secretly installed on the Web  
 6 Properties.

7           59. Plaintiff and Class Members did not intend or have any reason to suspect their  
 8 Private Information would be shared with Facebook or that MultiCare was tracking their  
 9 every movement and disclosing same to Facebook when they entered highly sensitive  
 10 information on the Web Properties.

11           60. MultiCare did not disclose to or warn Plaintiff or Class Members that MultiCare  
 12 used Plaintiff's and Class Members' Web Properties submissions for Facebook's marketing  
 13 purposes.

14           61. Plaintiff and Class Members never consented, agreed, authorized or otherwise  
 15 permitted MultiCare to disclose their Private Information to Meta.

16           62. On information and good faith belief, MultiCare's unauthorized disclosure is  
 17 not just limited to activity on the public-facing Website, but the disclosure also involved  
 18 information contained within the highly sensitive and private Patient Portal, which requires  
 19 patients to enter a specific login.

20           63. MultiCare disclosed to Meta the following non-public private information:

- 21           a. when a patient sets up or schedules an appointment;
- 22           b. when a patient registers for or logs into the Patient Portal;
- 23           c. when a patient seeks to pay their medical bills;
- 24           d. when a patient seeks to request copies of their medical records;
- 25           e. information that a patient types into or chooses on an appointment form;



- f. when a patient clicks a button to call the provider from a mobile device directly from the Website;
- g. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;
- h. the communications a patient exchanges through MultiCare's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including—upon information and belief—whether they are made while a patient is still logged in to the Patient Portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged into the Patient Portal; and
- i. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

64. MultiCare deprived Plaintiff and Class Members of their privacy rights when it:

- (1) implemented technology (i.e. Meta Pixels) that surreptitiously tracked, recorded and disclosed Plaintiff's and other Users' confidential communications and Private Information;
- (2) disclosed patients' protected information to Meta—an unauthorized third party and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.



2. **Meta’s Collection Tools Redirect Patients’ Data from MultiCare’s Web Properties to Facebook to Use for Ad Targeting.**

65. Facebook operates the world’s largest social media company and generated nearly \$117 billion in revenue in 2022, roughly 97% of which came from selling targeted advertising.<sup>19</sup>

66. As a core part of its business, Facebook maintains profiles on users that include the user’s real names, locations, email addresses, friends, likes and communications that Facebook associates with personal identifiers, including IP addresses, cookies, device identifiers and advertising ID identifiers.

67. Facebook also tracks non-Facebook users through its widespread internet marketing products and various tracking codes, such as the Meta Pixel, tracking scripts and cookies.

68. Facebook then sells advertising space by highlighting its ability to target users.<sup>20</sup> Facebook can target users so effectively because it surveils user activity both on and off its site.<sup>21</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”<sup>22</sup>

69. Facebook compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.<sup>23</sup>

70. Indeed, Facebook utilizes the precise type of information disclosed by MultiCare to identify, target, and market products and services to individuals.

<sup>19</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx> (last visited Jun. 12, 2024).

<sup>20</sup> WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706> (last visited Jun. 12, 2024).

<sup>21</sup> ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Jan. 12, 2024).

<sup>22</sup> AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Jun. 12, 2024).

<sup>23</sup> EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences> (last visited Jun. 12, 2024).

71. Advertisers can also build “Custom Audiences.”<sup>24</sup> Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”<sup>25</sup>

72. With Custom Audiences, advertisers can target existing customers directly, and they can also build “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”<sup>26</sup>

73. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences *only if they first supply Facebook with the underlying data*. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools.”<sup>27</sup>

74. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”<sup>28</sup>

75. Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

---

<sup>24</sup> ABOUT CUSTOM AUDIENCES,

<https://www.facebook.com/business/help/744354708981227?id=2469097953376494> (last visited Jun. 12, 2024).

<sup>25</sup> AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,

<https://www.facebook.com/business/ads/ad-targeting> (last visited Jun. 12, 2024).

<sup>26</sup> ABOUT LOOKALIKE AUDIENCES,

<https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited Jun. 12, 2024).

<sup>27</sup> CREATE A CUSTOMER LIST CUSTOM AUDIENCE,

<https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; Facebook, Create a Website Custom Audience <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last visited Jun. 12, 2024).

<sup>28</sup> THE FACEBOOK BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087> (last visited Jun. 12, 2024).

1           76. The Business Tools are automatically configured to capture certain data, like  
2 when a User visits a webpage, that webpage's Universal Resource Locator ("URL") and  
3 metadata, or when a user downloads a mobile application or makes a purchase.<sup>29</sup>

4           77. Facebook's Business Tools can also track other events. Facebook offers a menu  
5 of "standard events" from which advertisers can choose, including what content a visitor  
6 views or purchases.<sup>30</sup> Advertisers can even create their own tracking parameters by building a  
7 "custom event."<sup>31</sup>

8           78. One such Business Tool is the Meta Pixel. Facebook offers this code to  
9 advertisers, like MultiCare, to integrate into their website. As the name implies, the Meta  
10 Pixel "tracks the people and type of actions they take."<sup>32</sup>

11           79. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel  
12 "can help you better understand the effectiveness of your advertising and the actions people  
13 take on your site, like visiting a page or adding an item to their cart."<sup>33</sup>

14           80. Meta tells advertisers that the Meta Pixel will improve their Facebook  
15 advertising, including by allowing them to:

- 16           a. "measure cross-device conversions" and "understand how your cross-device  
17 ads help influence conversion";
- 18           b. "optimize the delivery of your ads" and "[e]nsure your ads reach the  
19 people most likely to take action" and

21  
22 <sup>29</sup> See FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED,  
23 <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR  
24 FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>;  
25 FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited  
26 Jun. 19, 2024).

27 <sup>30</sup> SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS,  
<https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited Jun. 19, 2024).

<sup>31</sup> ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also FACEBOOK, APP  
EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>. (last visited Jun. 19, 2024).

<sup>32</sup> RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Jun. 11, 2024).

<sup>33</sup> Meta, Meta Pixel (2023), <https://www.facebook.com/business/tools/meta-pixel>.

c. “create Custom Audiences from website visitors” and create “[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones.”<sup>34</sup>

81. Meta explains that the Meta Pixel “log[s] when someone takes an action on your website” such as “adding an item to their shopping cart or making a purchase,” and the user’s subsequent action:



Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in [Events Manager](#). From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

82. The Meta Pixel is customizable, meaning web developers can choose the actions the Pixel will track and measure.

83. Meta advises web developers to place the Meta Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:

---

<sup>34</sup> *Id.*

## Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing `<head>` tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your `<head>` tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

84. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.<sup>35</sup>

85. If a healthcare provider, such as MultiCare, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with his healthcare provider—traveling directly from the user's browser to Facebook's server.

86. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

87. This contemporaneous and secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by the Facebook code installed by MultiCare and concurrent with the Users' communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read the MultiCare's Web Properties— MultiCare's own code, and the Facebook code MultiCare embedded.

<sup>35</sup> Meta, *Meta Pixel* (2023), <https://www.facebook.com/business/tools/meta-pixel>.

1           88. Thus, the Meta “pixel allows Facebook to be a silent third-party watching  
2 whatever you’re doing.”<sup>36</sup>

3           89. MultiCare, through its installation and use of the Meta Pixel, disclosed to Meta  
4 the content of patient communications while its patients were exchanging communications  
5 with MultiCare’s Web Properties.

6           90. MultiCare’s use of the Meta Pixel to send Facebook the names and/or specialty  
7 of patients’ doctors or their appointment-related details would have permitted MultiCare to  
8 specifically target its existing patients with Facebook ads *based on their health conditions*, as  
9 well as create Lookalike Audiences for the same purpose. This could only be accomplished by  
10 MultiCare disclosing to Meta the content of those patients’ communications on MultiCare’s  
11 Web Properties, providing Facebook with a list of MultiCare’s patients, or otherwise  
12 disclosing the identity of MultiCare’s patients to Meta through the Meta Collection Tools.

13           **3. MultiCare Improperly Disclosed Plaintiff’s & Class Members’ Private**  
14           **Information to Google.**

15           91. MultiCare utilized Google advertisements and intentionally installed the Google  
16 Collection Tools on its Web Properties, including but not limited to Google Analytics, Google  
17 Tag Manager, and DoubleClick Ad trackers.

18           92. MultiCare installed a Google Analytics tracker, Google Tag Manager, and  
19 DoubleClick Ad trackers beginning in at least May 2008 and continued to disclose its  
20 patient’s data to Google through at least June 30, 2024.

21           93. Google offers an ad targeting option called “Custom Audiences.” When a  
22 patient takes an action on a Google healthcare Partner’s website embedded with Google  
23 tracking code, the tracking code will be triggered to send Google “Event” data that Google  
24 matches to its Users. A web developer can then create a “Custom Audience” based on Events  
25

---

26 <sup>36</sup> Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows*  
27 *everything*, USA Today (March 4, 2020 4:52 am), <https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#>.

1 to target ads to those patients. The Google tracking code can then be used to measure the  
2 effectiveness of an advertising campaign.<sup>37</sup>

3 94. When Plaintiff and Class Members sought and used MultiCare's Web  
4 Properties, their Private Information was intercepted concurrently in real time and then  
5 disseminated to Google and potentially to other third parties, via the Google tracking code and  
6 other Google Collection Tools that MultiCare secretly installed on the Web Properties.

7 95. Plaintiff and Class Members did not intend or have any reason to suspect their  
8 Private Information would be shared with Google or that MultiCare was tracking their every  
9 movement and disclosing same to Google when they entered highly sensitive information on  
10 MultiCare's Web Properties.

11 96. MultiCare did not disclose to or warn Plaintiff or Class Members that MultiCare  
12 used Plaintiff's and Class Members' Web Properties submissions for Google's marketing  
13 purposes.

14 97. Plaintiff and Class Members never consented, agreed, authorized or otherwise  
15 permitted MultiCare to disclose their Private Information to Google.

16 98. MultiCare's unauthorized disclosure is not just limited to activity on the public  
17 Website, but the disclosure also involved information contained within the highly sensitive  
18 and private Patient Portal, which requires patients to enter a specific login.

19 99. MultiCare disclosed to Google the following non-public private information:

- 20 a. Details about users' activities on MultiCare's Web Properties;
- 21 b. The exact date, time, and location from which a user first entered  
22 MultiCare's Web Properties at <https://www.multicare.org>;
- 23 c. Information that a user is actively on MultiCare's homepage, and each  
24 subsequent click on MultiCare's Web Properties is transmitted to  
25 Google;

26 <sup>37</sup> Google Ads API, *Custom Audiences*, [https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how\\_custom\\_audiences\\_work](https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how_custom_audiences_work) (last visited May 29, 2024)  
27



- d. Keyword searches, Location, and Physician Searches;
- e. Appointment scheduling activities;
- f. when a patient clicks to sign up for the Patient Portal;
- g. when a patient clicks to log in to the Patient Portal;
- h. when a patient seeks to pay their medical bills;
- i. when a patient seeks to request copies of their medical records;
- j. when a patient views MultiCare's services related to specific conditions;
- and
- k. other activities that reveal users' patient status.

100. Further, the data from 'events' captured by Defendant's Google Analytics tracker shows that MultiCare has not enabled IP Masking and transmits user IP addresses to Google alongside their PHI.

101. MultiCare deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (*i.e.*, Google Collection Tools) that surreptitiously tracked, recorded and disclosed Plaintiff's and other Users' confidential communications and Private Information; (2) disclosed patients' protected information to Google—an unauthorized third party and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

**4. Google's Collection Tools Redirect Patients' Data from MultiCare's Web Properties to Google to Use for Ad Targeting.**

102. Google operates the world's largest internet search engine company and generated roughly \$307 billion in revenue in 2023, roughly 76% of which came from selling advertising.<sup>38</sup>

---

<sup>38</sup> ALPHABET, INC REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS, <https://abc.xyz/assets/95/eb/9cef90184e09bac553796896c633/2023q4-alphabet-earnings-release.pdf> (last visited May 29, 2024).



103. As a core part of its business, Google maintains profiles on users of its products (e.g., Gmail, Google Search, Chrome browser, YouTube or Google devices) that include the user's real names, locations, email addresses, friends, internet activity, and communications that Google associates with personal identifiers, including IP addresses, cookies, device identifiers and advertising ID identifiers.

104. Google also tracks people regardless of whether they use Google products through its widespread internet marketing products and ubiquitous trackers.

105. Google then sells advertising space by highlighting its ability to target users.<sup>39</sup> Google can target users so effectively because it surveils user activity both on and off Google sites and apps. This allows Google to make inferences about users beyond what they explicitly disclose, determining audiences by "[users'] activity using Google products and third-party websites, or estimated based on content certain groups of people are likely to be interested in."<sup>40</sup>

106. Google compiles this information into a generalized dataset called "Audience Segments," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.<sup>41</sup>

107. Indeed, Google utilizes the precise type of information disclosed by MultiCare to identify, target, and market products and services to individuals.

108. Advertisers can also select "Custom Audiences."<sup>42</sup> Custom Audiences enable advertisers to reach "your ideal audience by entering relevant keywords, URLs, and apps."<sup>43</sup>

<sup>39</sup> BENEFITS OF ONLINE ADVERTISING AND GOOGLE ADS, <https://support.google.com/google-ads/answer/6123875?hl=en#:~:text=Control%20your%20costs,per%20day%2C%20and%20per%20ad.> (last visited May 29, 2024).

<sup>40</sup> ABOUT AUDIENCE SEGMENTS, <https://support.google.com/google-ads/answer/2497941?sjid=6716156162402223675-NA> (last visited May 29, 2024).

<sup>41</sup> *Id.*

<sup>42</sup> CUSTOM AUDIENCES, [https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how\\_custom\\_audiences\\_work](https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how_custom_audiences_work) (last visited June 12, 2024).

<sup>43</sup> *Id.*

109. With Custom Audiences, advertisers can target existing customers directly, and they can also build Audiences similar to their existing customers.

110. As Google puts it, the Google Analytics “Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business.”<sup>44</sup>

111. Put more succinctly, Google Analytics, Google Tag Manager and DoubleClick are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Google to intercept and collect user activity on those platforms.

112. Google Analytics is automatically configured to capture certain data, like when a User visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.<sup>45</sup>

113. Google Analytics can also track other events. Google offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases.<sup>46</sup> Advertisers can even create their own tracking parameters by building a “custom event.”<sup>47</sup>

114. Google offers this code to advertisers, like MultiCare, to integrate into their website. Google Analytics tracks “how many users perform the action and evaluate marketing performance across all channels that lead users to perform the action... A key event is an event that measures an action that's particularly important to the success of your business. When someone triggers the event by performing the action, the key event is recorded in Google Analytics and surfaced in your Google Analytics reports.”<sup>48</sup>

<sup>44</sup> HOW GOOGLE ANALYTICS WORKS, <https://support.google.com/analytics/answer/12159447?hl=en> (last visited May 29, 2024).

<sup>45</sup> GOOGLE ANALYTICS – THE FINER POINTS <https://marketingplatform.google.com/about/analytics/features/> (last visited May 29, 2024).

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> GOOGLE ANALYTICS HELP - ABOUT KEY EVENTS, <https://support.google.com/analytics/answer/9267568?hl=en> (last visited May 29, 2024).

1 115. Google pushes advertisers to install Google Analytics. Google says Analytics  
2 “can track what online behavior led to purchases and use that data to make informed decisions  
3 about how to reach new and existing customers.”<sup>49</sup>

4 116. Google tells advertisers that Google Analytics will improve their Google  
5 advertising through the following features:

- 6 a. “Collects both website and app data to better understand the customer  
7 journey;
- 8 b. Uses event-based data instead of session-based;
- 9 c. Includes privacy controls such as cookieless measurement, and  
10 behavioral and key event modeling;
- 11 d. Predictive capabilities offer guidance without complex models;
- 12 e. Direct integrations to media platforms help drive actions on your  
13 website or app.”<sup>50</sup>

14 117. Google explains that Google Analytics logs consumer actions, such as clicking  
15 a button, called “events”.<sup>51</sup>

16  
17  
18  
19  
20  
21  
22  
23  
24 <sup>49</sup> GOOGLE ANALYTICS HELP – THE VALUE OF DIGITAL ANALYTICS,  
25 [https://support.google.com/analytics/answer/12159453?hl=en&sjid=8517741530658858223-](https://support.google.com/analytics/answer/12159453?hl=en&sjid=8517741530658858223-NA&visit_id=638526037873608158-2523537901&rd=2&ref_topic=14089939)  
26 [NA&visit\\_id=638526037873608158-2523537901&rd=2&ref\\_topic=14089939](https://support.google.com/analytics/answer/12159453?hl=en&sjid=8517741530658858223-NA&visit_id=638526037873608158-2523537901&rd=2&ref_topic=14089939) (last visited May 29, 2024).

27 <sup>50</sup> GOOGLE ANALYTICS HELP – SET UP ANALYTICS FOR A WEBSITE AND/OR APP  
<https://support.google.com/analytics/answer/9304153?sjid=8517741530658858223-NA> (last visited May 29,  
2024).

<sup>51</sup> *Id.*

## How it works

Let's say someone clicks a link on your tagged website that takes them to an external website. The following illustrates what happens when the user clicks the link:



1

The user visits your website and clicks a link to an external website



2

Analytics receives the click event and surfaces the event and parameters in the Realtime report



3

Analytics fully processes the event



4

Analytics surfaces the data in dimensions and metrics used in reports, audiences, etc.

118. According to Google, “An event allows you to measure a specific interaction or occurrence on your website or app. For example, you can use an event to measure when someone loads a page, clicks a link, or completes a purchase, or to measure system behavior, such as when an app crashes or an impression is served.”<sup>52</sup>

119. The Google Analytics tracker is customizable. Meaning, web developers can choose the events Google Analytics will track and measure.

120. Google advises web developers to place Google tracking code early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.<sup>53</sup>

<sup>52</sup> ABOUT EVENTS, <https://support.google.com/analytics/answer/9322688?hl=en#zippy=%2Crealtime-report%2Cdebugview-report> (last visited May 29, 2024).

<sup>53</sup> GOOGLE ANALYTICS HELP – SET UP ANALYTICS FOR A WEBSITE AND/OR APP, <https://support.google.com/analytics/answer/9304153?hl=en#zippy=%2Cadd-the-google-tag-directly-to-your-web-pages> (last visited May 29, 2024).



## Set up data collection for websites

To begin seeing data in your new Google Analytics 4 property, you'll need to do one of the following:

Add the tag to a website builder or CMS-hosted website (e.g., HubSpot, Shopify, etc.) 

Add the Google tag directly to your web pages 

You need access to the HTML for your web pages. Ask your web developer to perform these steps if you're unable to complete the steps yourself.


1. Sign in to your [Google Analytics account](#) .
2. Click [Admin](#) .
3. At the top of the *Property* column, select your property.
4. In the *Property* column, click **Data streams > Web**.
5. Click the data stream for your website.
6. Under *Google tag*, click **View tag instructions**.
7. On the *Installation instructions* page, select **Install manually**:
  - On the screen, you'll see the JavaScript snippet for your account's Google tag. Your Google tag is the entire section of code that appears, beginning with:

```
<!-- Google tag (gtag.js) -->
```

and ending with

```
</script>
```

Paste your Google tag immediately after the `<head>` on each page of your website.

Data collection may take up to 30 minutes to begin. You can then use the [Realtime report](#)  to verify that you're receiving data.

121. Google also provides advertisers with step-by-step instructions for setting up and installing Google tracking code on their website, so that companies can add Google tracking code to their website without a developer.<sup>54</sup>

122. If a healthcare provider, such as MultiCare, installs Google Analytics code as Google recommends, patients' actions on the provider's website are contemporaneously redirected to Google. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Google's source code commands the patient's computing device to

<sup>54</sup> *Id.*

1 send the content of the patient’s communication to Google while the patient is communicating  
2 with his healthcare provider—traveling directly from the user’s browser to Google’s server.

3 123. In other words, by design, Google receives the content of a patient’s portal log  
4 in communication immediately when the patient clicks the log-in button—even before the  
5 healthcare provider receives it.

6 124. This contemporaneous, and secret transmission contains the original GET  
7 request sent to the host website, along with additional data that Google Analytics is  
8 configured to collect. This transmission is initiated by the Google code installed by MultiCare  
9 and concurrent with the Users’ communications with the host website. Two sets of code are  
10 thus automatically run as part of the browser’s attempt to load and read MultiCare’s Web  
11 Properties— MultiCare’s own code, and the Google code MultiCare embedded.

12 125. MultiCare, through its installation and use of Google Analytics, disclosed to  
13 Google the content of patient communications while its patients were exchanging  
14 communications with MultiCare’s Web Properties.

15 126. MultiCare’s use of Google Analytics to send Google the names of patients’  
16 doctors would have permitted MultiCare to specifically target its existing patients with  
17 Google ads *based on their health conditions*, as well as create Audiences for the same  
18 purpose. This could only be accomplished by MultiCare disclosing to Google the content of  
19 those patients’ communications on MultiCare’s Web Properties, providing Google with a list  
20 of MultiCare’s patients, or otherwise disclosing the identity of MultiCare’s patients to Google  
21 through Google Analytics.

22 **5. MultiCare’s Use of Source Code, Google Analytics, Meta Trackers &**  
23 **Interception of HTTP Requests.**

24 127. Web browsers are software applications that allow consumers to navigate the  
25 web and view and exchange electronic information and communications over the Internet.  
26 Each “client device” (such as a computer, tablet or smartphone) accesses web content through  
27

1 a web browser (e.g., Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft's  
2 Edge).

3 128. Every website is hosted by a computer "server" that holds the website's  
4 contents and through which the entity in charge of the website exchanges communications  
5 with Internet users' client devices via web browsers.

6 129. Web communications consist of HTTP Requests and HTTP Responses, and any  
7 given browsing session may consist of thousands of individual HTTP Requests and HTTP  
8 Responses, along with corresponding cookies:

9 • **HTTP Request:** an electronic communication sent from the client  
10 device's browser to the website's server. GET Requests are one of the most  
11 common types of HTTP Requests. In addition to specifying a particular  
12 URL (i.e., web address), GET Requests can also send data to the host server  
embedded inside the URL, and can include cookies.

13 • **Cookies:** a small text file that can be used to store information on  
14 the client device which can later be communicated to a server or servers.  
15 Cookies are sent with HTTP Requests from client devices to the host server.  
16 Some cookies are "third-party cookies" which means they can store and  
communicate data when visiting one website to an entirely different  
website.

17 • **HTTP Response:** an electronic communication that is sent as a  
18 reply to the client device's web browser from the host server in response to  
an HTTP Request. HTTP Responses may consist of a web page, another  
kind of file, text information, or error codes, among other data.<sup>55</sup>

19 130. A patient's HTTP Request essentially asks the Website to retrieve certain  
20 information (such as the name of a doctor with whom a patient makes an appointment), and  
21 the HTTP Response renders or loads the requested information in the form of "Markup" (the  
22 pages, images, words, buttons, and other features that appear on the patient's screen as they  
23 navigate the Web Properties).

24  
25  
26 <sup>55</sup> One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP  
27 Responses.



1           131. Every website is comprised of Markup and “Source Code.” Source Code is a set  
2 of instructions that commands the website visitor’s browser to take certain actions when the  
3 web page first loads or when a specified event triggers the code.

4           132. Source code may also command a web browser to send data transmissions to  
5 third parties in the form of HTTP Requests quietly executed in the background without  
6 notifying the web browser’s user. The Google and Meta Collection Tools and other tracking  
7 technologies MultiCare uses constitute source code that does just that. These tracking  
8 technologies thus act much like a traditional wiretap.

9           133. MultiCare encourages customers to use its Web Properties to obtain healthcare  
10 services, such as making appointments with doctors and other providers and take other actions  
11 related to their personal health care. When interacting with MultiCare’s Web Properties like  
12 this, Plaintiff and Class Members convey highly private and sensitive information to  
13 MultiCare.

14           134. When patients visit MultiCare’s Web Properties via an HTTP Request to  
15 MultiCare’s server, that server sends an HTTP Response including the Markup that displays  
16 the webpage visible to the user and Source Code, including MultiCare’s Google and Meta  
17 Collection Tools.

18           135. Thus, MultiCare is in essence handing patients a tapped device, and once the  
19 webpage is loaded into the patient’s browser, the software-based wiretap is quietly waiting for  
20 private communications on the Web Properties to trigger the tap, which intercepts those  
21 communications intended only for MultiCare and transmits those communications to third  
22 parties, including Google and Meta.

23           136. MultiCare intentionally configured the Google and Meta Collection Tools  
24 installed on the Web Properties to capture both the “characteristics” of individual patients’  
25 communications with the MultiCare’s Web Properties (e.g., their IP addresses, Facebook ID,  
26 cookie identifiers, device identifiers and account numbers) and the “content” of these  
27



communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

**6. Google and Meta Use Unique Identifiers to Match the Health Information They Collect with Google and Facebook Users.**

137. Meta uses cookies to identify patients, including cookies named c\_user, datr, fr, and \_fbp.

138. The c\_user cookie identifies Facebook users. The c\_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one—and only one—unique c\_user cookie. Meta uses the c\_user cookie to track each user’s activities and communications.

139. An unskilled computer user can obtain the c\_user cookie value for any Facebook user by (1) going to the user’s Facebook page, (2) right-clicking with their mouse, (3) selecting “View page source,” (4) executing a control-f function for “UserID,” and (5) copying the number value that appears after “UserID” in the page source code of the Facebook user’s page.

140. Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing www.facebook.com/4 into a browser and hitting enter, a browser directs to Mr. Zuckerberg’s page at www.facebook.com/zuck.

141. A user’s Facebook ID is therefore linked to their Facebook profile, which contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user’s Facebook ID uniquely identifies an individual’s Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user’s corresponding Facebook profile. To find the Facebook account associated with a c\_user cookie, one simply needs to type www.facebook.com/ followed by the c\_user ID.

1 142. The Meta datr cookie identifies the web browser the patient is using. It is an  
 2 identifier unique to each patient's specific web browser, so it is another way Meta can identify  
 3 Facebook users.

4 143. Meta keeps a record of every datr cookie identifier associated with each of its  
 5 users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or  
 6 his Facebook account from Meta by using the Facebook "Download Your Information" tool.

7 144. The Meta fr cookie is an encrypted combination of the c\_user and datr  
 8 cookies.<sup>56</sup>

9 145. The c\_user, datr and fr cookies are traditional third-party cookies, meaning they  
 10 are cookies associated with a party other than the entity with which a person is  
 11 communicating at the time. In the case of MultiCare, they are third-party cookies because  
 12 Meta is a third party to the communication between a patient and their healthcare provider.

13 146. The Meta \_fbp cookie is a Facebook identifier that is set by Facebook source  
 14 code and associated with the healthcare provider using the Meta Pixel.

15 147. The \_fbp cookie is a third-party cookie in that it is also a cookie associated with  
 16 Meta that is used by Meta to associate information about a person and their communications  
 17 with non-Meta entities while the person is on a non-Meta website or application.

18 148. Meta disguises the \_fbp cookie as a first-party cookie even though it is Meta's  
 19 cookie on non-Meta websites.

20 149. By disguising the \_fbp cookie as a first-party cookie for a healthcare provider  
 21 rather than a third-party cookie associated with Facebook, Meta ensures that the \_fbp cookie  
 22 is placed on the computing device of patients who seek to access the patient portal.

23 150. Healthcare providers with a patient portal require patients to enable first-party  
 24 cookies to gain access to their patient records through the portal.

25 \_\_\_\_\_  
 26 <sup>56</sup> See Gunes Acar, *et al.*, *Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the*  
 27 *Belgian Privacy Commission* (Mar. 27, 2015), [https://securehomes.esat.kuleuven.be/~gacar/fb\\_tracking/fb\\_pluginsv1.0.pdf](https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

1           151. The purpose of these portal-associated first-party cookies is security. The \_fbp  
2 cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action  
3 to delete or clear third-party cookies from their device, the \_fbp cookie is not impacted—even  
4 though it is a Meta cookie—again, because Meta has disguised it as a first-party cookie. Meta  
5 also uses IP address and user-agent information to match the health information it collects  
6 from Meta healthcare Partners with Facebook users.

7           152. Google uses similar tools to track users of websites with Google tracking code  
8 installed, such as Google Analytics.

9           153. From at least May 9, 2008, MultiCare installed Google Analytics.

10          154. Universal Analytics tracks, among other types of data, “events” which include  
11 instances when a patient downloads a document, engages with a webpage by putting in their  
12 login information, or navigates to a certain part of the webpage and clicks a button.

13          155. For these Universal Analytics events, MultiCare needed to opt-in to IP Masking  
14 to stop Google from collecting users’ IP addresses. Plaintiff’s investigation to-date indicates  
15 that, based on the absence of an “aip=1” parameter in Defendant’s Universal Analytics events,  
16 MultiCare did not enable IP Masking. Consequently, Google collected and stored IP addresses  
17 from MultiCare users.

18          156. Google DoubleClick events are also linked to Universal Analytics events. Each  
19 DoubleClick event includes the Universal Analytics event’s ‘tid’. The ‘tid’ is the tag ID of the  
20 Universal Analytics tracking code used by MultiCare, and it's how Google identifies  
21 MultiCare’s Google Analytics account.

22          157. Each DoubleClick event also includes the ‘cid’ parameter. The ‘cid’ parameter  
23 is a first-party cookie that helps Google identify MultiCare’s users. Consequently, Google  
24 can connect DoubleClick and Universal Analytics events with individual users of MultiCare’s  
25 Web Properties.  
26  
27

158. A first-party cookie, unique to MultiCare’s Website, differs from third-party cookies in that it will not be identical when a user visits another website.

159. Accordingly, MultiCare’s Web Properties through the Google and Meta Collection Tools and other tracking technologies routinely provide Facebook and Google with MultiCare’s patients’ unique personal identifiers, including Facebook IDs, Google “cid” cookies, IP addresses, and/or device IDs and the other information they input into the Web Properties, including not only their medical searches, treatment requests, and the webpages they view. This is precisely the type of identifying information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.<sup>57</sup> Plaintiff’s and Class Members’ identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

160. After intercepting and collecting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the user’s Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

161. While the Meta Pixel tool “hashes” personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent Facebook from reading, understanding, and using the data.<sup>58</sup>

162. In fact, Facebook explicitly uses the hashed information it gathers to link Pixel-transmitted data to Facebook profiles.<sup>59</sup> Indeed, there would be no value in targeting Facebook

---

<sup>57</sup> *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Jun. 19, 2024).

<sup>58</sup> See <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>;

<https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142>.

<sup>59</sup> See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

1 users with MultiCare’s ads if Facebook couldn’t read the hashed data it received from  
2 MultiCare to know *who* to target.

3 163. As Facebook explains, “[a]utomatic advanced matching will tell your pixel to  
4 look for recognizable form fields and other sources on your website that contain information  
5 such as first name, last name and email address. The Meta Pixel receives that information  
6 along with the event, or action, that took place. This information gets hashed in the visitor's  
7 browser. ***We can then use the hashed information to more accurately determine which***  
8 ***people took action in response to your ad.***”<sup>60</sup>

9 164. Similarly, Facebook tells businesses: “When you upload your customer list in  
10 Ads Manager to create a Custom Audience, the information in your list is hashed before it’s  
11 sent to Facebook. ***Facebook uses this hashed information and compares it to our own***  
12 ***hashed information. Then, we help build your audience by finding the Facebook profiles***  
13 ***that match and create a Custom Audience for you from those matches.***”<sup>61</sup>

14 165. In other words, Facebook uses its own secret language to encode and then read  
15 and match individuals’ information.

16 166. Facebook claims that after hashing individuals’ Private Information (including  
17 their personal identifiers and PHI shared by Defendant) and matching it to Facebook profiles  
18 to create Custom Audiences, Facebook deletes the hashed data.

19 167. Even assuming this is true, by that point, the damage is done—Facebook has  
20 read, understood, analyzed, and expressly taken action to match the shared PHI with specific  
21 individuals, with the express purpose of targeting those individuals with ads based on the data  
22 (PHI) that was shared and used to create MultiCare’s Custom Audiences—all at MultiCare’s  
23 request.

26 <sup>60</sup> <https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142>.

27 <sup>61</sup> <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>.

168. Google uses a similar process to identify specific users and match their profiles with data collected by Google tracking code, such as Google Analytics, including specific actions taken by patients on websites in which Google tracking code is installed.

169. This disclosed PHI and PII allows Facebook and Google to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting MultiCare to target those persons with MultiCare's ads, Facebook and Google also then sell that information to marketers who will online target Plaintiff and Class Members.

**7. MultiCare Installed Meta Pixels on its Web Properties and Used the Meta Pixels to Transmit Private Information to Meta.**

170. Review of the archives of MultiCare's Web Properties shows that MultiCare installed Meta Pixels with ID 293179364212674 ("Meta Pixel 1"), ID 1830203120542010 ("Meta Pixel 2"), and ID 2560446094169142 ("Meta Pixel 3").

171. MultiCare installed Meta Pixel 1 as early as December 10, 2014. By October 28, 2016, MultiCare installed Meta Pixel 2, and sometime before November 25, 2020, MultiCare installed Meta Pixel 3.

172. The Pixels transmitted several types of "events" to Facebook with data disclosing Users' activities on the Web Properties, including PageView, Microdata and SubscribedButtonClick events. MultiCare began tracking Users' activities from the moment they arrived on MultiCare's homepage, <https://www.multicare.org/>. As Users navigated beyond the homepage, MultiCare continued to disclose user data including Users': (i) search activities such as exact search terms entered into the search bar, physicians sought (including their name and specialty), and MultiCare locations, (ii) classes and events browsing activities, (iii) bill pay activities, and (iv) other activities that reveal their patient status.

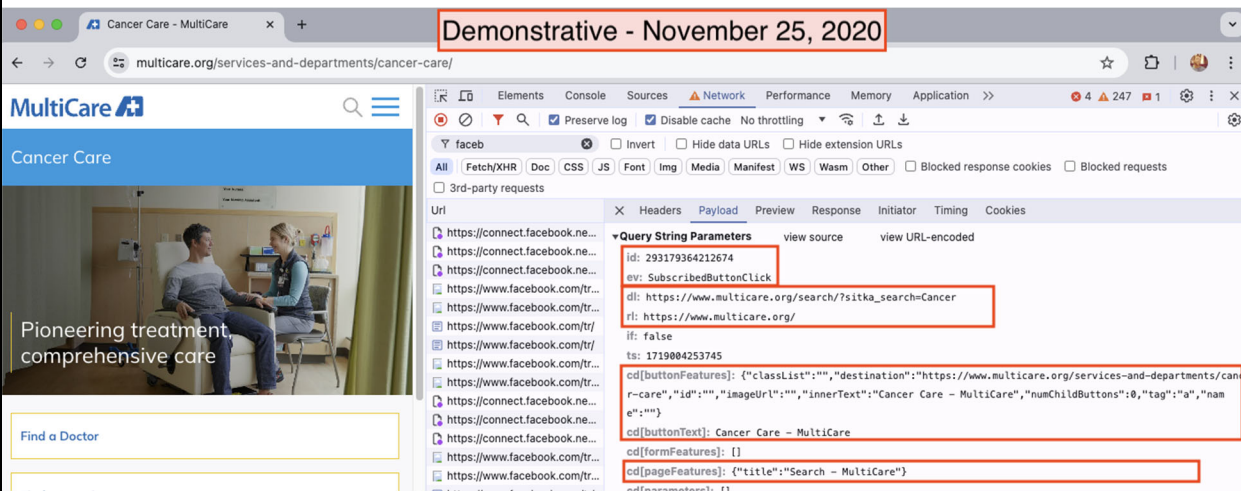
173. In each of the transmitted Meta Pixel events, MultiCare included the "c\_user" cookie, which Facebook uses to identify Users.

174. Therefore, Facebook could connect the cookie data that MultiCare transmitted with specified Users.

175. For example, when a User searched MultiCare's Web Properties to search for a doctor using the filters offered by Defendant, MultiCare Pixels transmitted the details of such searches to Facebook, including the doctor's specialty (e.g., "oncology"), to doctor's name (e.g., "Steven P. Register, MD"), provider's proximity to the User (by city and/or zip code), and types of insurance accepted by that provider.

176. If a User utilized Defendant's search bar, MultiCare disclosed specific search terms to Facebook, including medical conditions and/or treatments sought (e.g., searches for "cancer").

177. MultiCare continued to disclose the User's activities as they interacted with their search results. For instance, if the user clicked and loaded MultiCare's "Cancer Care" and/or "Breast Cancer" pages from their cancer search results, MultiCare would send that data to Facebook via SubscribedButtonClick, PageView, and Microdata events.





## ▼ Form Data view source view URL-encoded

id: 293179364212674

ev: Microdata

dl: https://www.multicare.org/services-and-departments/cancer-care/

rl: https://www.multicare.org/search/?sitka\_search=Cancer

if: false

ts: 1719004257132

cd[DataLayer]: []

```
cd[Meta]: {"title":"Cancer Care - MultiCare","meta:description":"The MultiCare Cancer Institute offers a combination of cancer expertise, treatment options and compassionate support that is personalized to meet your needs."}
```

```
cd[OpenGraph]: {"og:locale":"en_US","og:type":"article","og:title":"Cancer Care - MultiCare","og:description":"The MultiCare Cancer Institute offers a combination of cancer expertise, treatment options and compassionate support that is personalized to meet your needs.","og:url":"https://www.multicare.org/services-and-departments/cancer-care/","og:site_name":"MultiCare","article:publisher":"https://www.facebook.com/multicarehealthsystem","article:modified_time":"2024-05-21T23:13:22+00:00","og:image":"https://res.cloudinary.com/derwl0zbi/image/upload/v1698777281/mc-prd/TG-cancer-center-05-24-2023.jpg","og:image:width":"2560","og:image:height":"1707","og:image:type":"image/jpeg"}
```

178. If the User sought out specific services offered by MultiCare, that data was shared with Facebook (and Google) as well.

179. For example, Users can utilize Defendant's "Breast Cancer" page to take a breast cancer assessment, learn about biopsies and cancer treatments, and schedule a mammogram. MultiCare informed Facebook when a User clicked to perform each of these activities, via a SubscribedButtonClick event (see example below).

Demonstrative - November 25, 2020

Breast Cancer Risk Assessment

MultiCare

Learn your five-year and lifetime risk of breast cancer

Network

Query String Parameters

id: 293179364212674

ev: SubscribedButtonClick

dl: https://www.multicare.org/services-and-departments/cancer-care/diagnosis-evaluation/breast-cancer/

rl: https://www.multicare.org/services-and-departments/cancer-care/

if: false

ts: 1719004362277

cd[buttonFeatures]: {"classList":"btn btn--solid wpel-icon-right","destination":"https://profilers.evaliahealth.com/v3/ecd3da4c-d91b-4d40-a8e2-50c461832f05/?utm\_source=MCwebsite&utm\_medium=Website&utm\_campaign=breast-cancer-assessment&utm\_id=MultiCare-Website-EvaliaHealthLinks","id":"","imageUrl":"","innerText":"Begin Assessment","numChildButtons":0,"tag":"a","name":""}

cd[buttonText]: Begin Assessment

cd[formFeatures]: {}

cd[pageFeatures]: {"title":"Breast Cancer - MultiCare"}



180. When the User used Defendant's Web Properties schedule a mammogram, MultiCare would also disclose this information via a SubscribedButtonClick event. Next, as the scheduling page loaded, MultiCare would send Pageview and Microdata events informing Facebook that the user was on a page for "medical-imaging/mammography/."

181. From the "Mammography" page, users could schedule a mammogram by calling MultiCare or logging into MyChart. MultiCare would send a SubscribedButtonClick event for each activity, reporting to Facebook that the user clicked a button to call MultiCare or clicked to "Log in to MyChart to Schedule" while they were on the "3D Mammography – MultiCare" page (see example below).

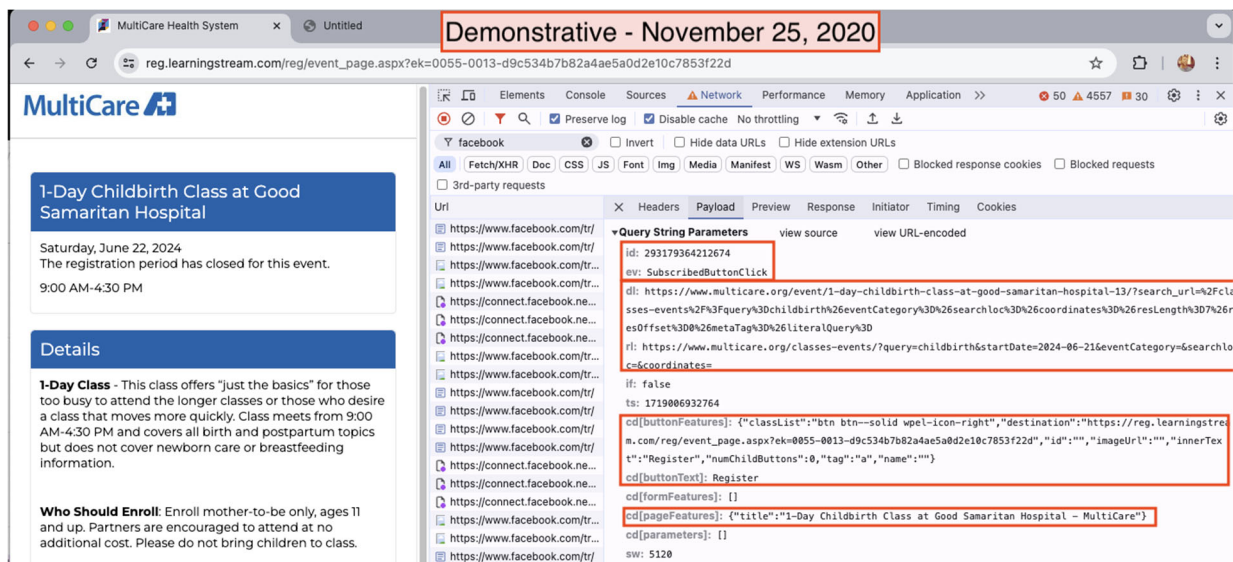
▼ Query String Parameters view source view URL-encoded

```

id: 293179364212674
ev: SubscribedButtonClick
dl: https://www.multicare.org/services-and-departments/medical-imaging/mammography/
rl: https://www.multicare.org/services-and-departments/cancer-care/diagnosis-evaluation/breast-cancer/
if: false
ts: 1719004694705
cd[buttonFeatures]: {"classList": "btn btn--solid", "destination": "https://mychart.multicare.org/mymulticare/Authentication/Login?", "id": "", "imageUrl": "", "innerText": "Log in to MyChart to Schedule", "numChildButtons": 0, "tag": "a", "name": ""}
cd[buttonText]: Log in to MyChart to Schedule
cd[formFeatures]: []
cd[pageFeatures]: {"title": "3D Mammography – MultiCare"}

```

182. Further, MultiCare Website provides patients with an option to search for and register for healthcare related classes. When a User utilized this function, MultiCare informed Facebook and Google about every step a User took, from the specific searches they conducted (e.g., "query=childbirth"), the date of the class chosen, the exact title of the class and its location (e.g., "1-Day Childbirth Class at Good Samaritan Hospital"), additional class details (e.g., "Class meets from 9:00 AM-4:30 PM and covers all birth and postpartum topics"), and the fact that the User registered for the class (see example below):



183. Just like with other sensitive PHI disclosed by MultiCare to Facebook in other examples herein, this data was sent along with the User's unique personal identifiers including their c\_user Facebook ID, allowing Facebook to learn that the person in question was pregnant – and utilize that information for targeted advertising.

184. Similarly sensitive PHI concerning healthcare classes and Users' PII was sent by MultiCare to Google.

## 8. MultiCare Installed Google Collection Tools on its Web Properties and Used Google Analytics to Transmit Private Information to Google.

185. A review of MultiCare's Web Properties shows that starting no later than November 9, 2015, MultiCare configured and installed a Google Tag Manager "container" with ID GTM-NMDGH4 ("GTM1").

186. Archives of GTM1's configuration files demonstrate the actions that MultiCare took using the Google tracking code that it installed and the custom events that it set up to transmit patients' Private Information to Google.

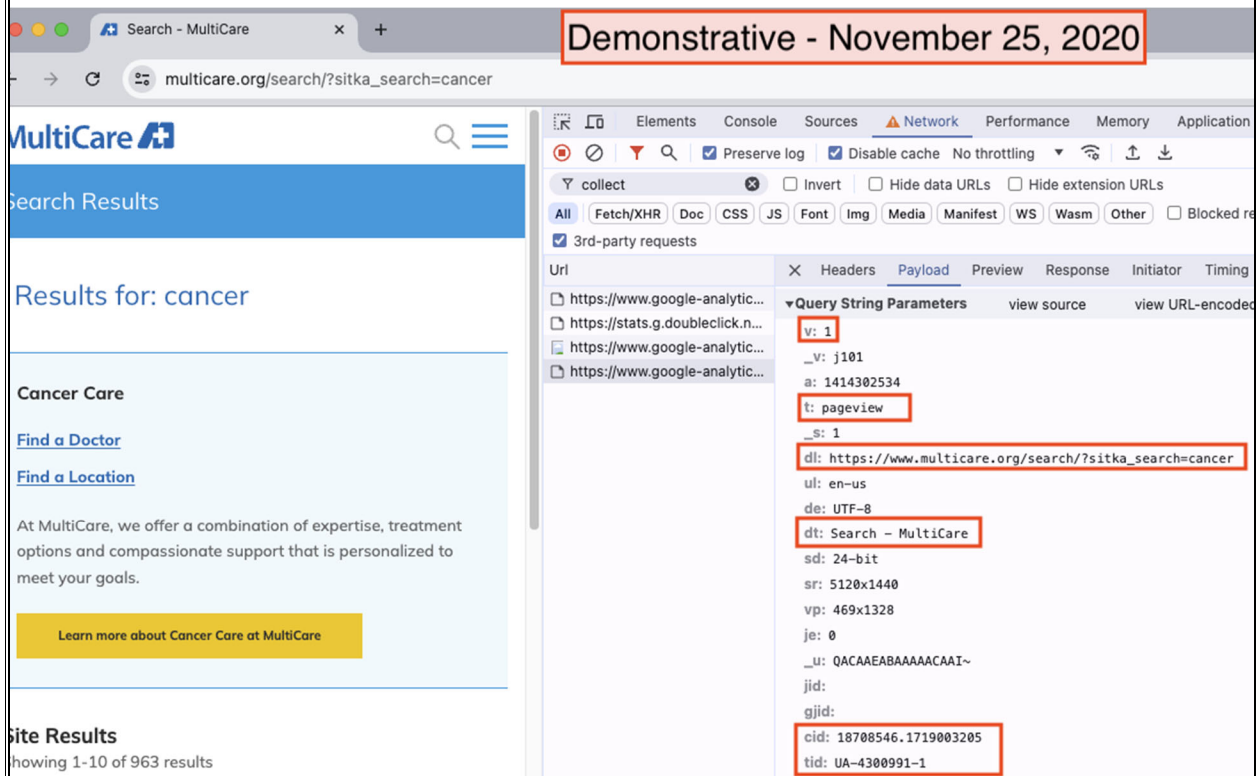
187. Using the Google tracking code installed on its Web Properties, MultiCare transmitted "Pageview," "Click," "Phone" and "DoubleClick" events that track Users' activities, starting with a User's arrival on MultiCare's homepage.



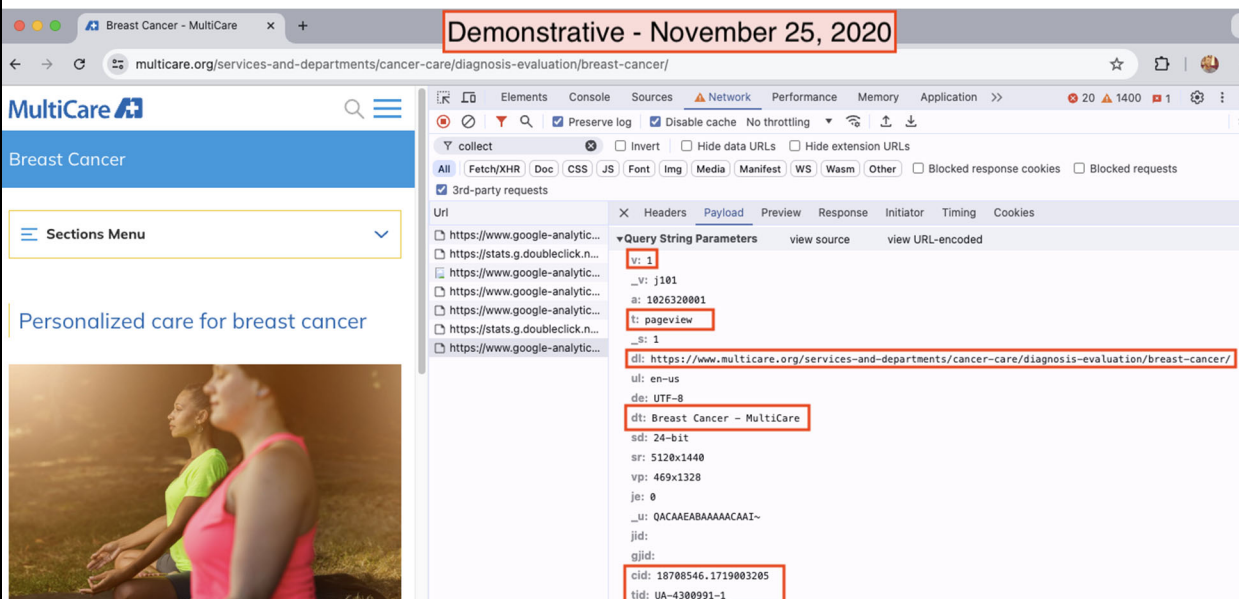
188. As Users navigated beyond the homepage, MultiCare continued to disclose user data including Users': (i) search activities, (ii) classes and events browsing activities, (iii) bill pay activities, and (iv) other activities that reveal their patient status.

189. With respect to the GTM1 Configuration shown above, UA1 signifies a Universal Analytics event, as indicated by its ID beginning with "UA-". For these Universal Analytics events, MultiCare needs to opt-in to "IP Masking" to stop Google from collecting users' IP addresses. The absence of an 'aip=1' parameter in the UA1 events indicates that MultiCare has not enabled IP Masking. Consequently, Google collected and stored IP addresses from MultiCare Users.

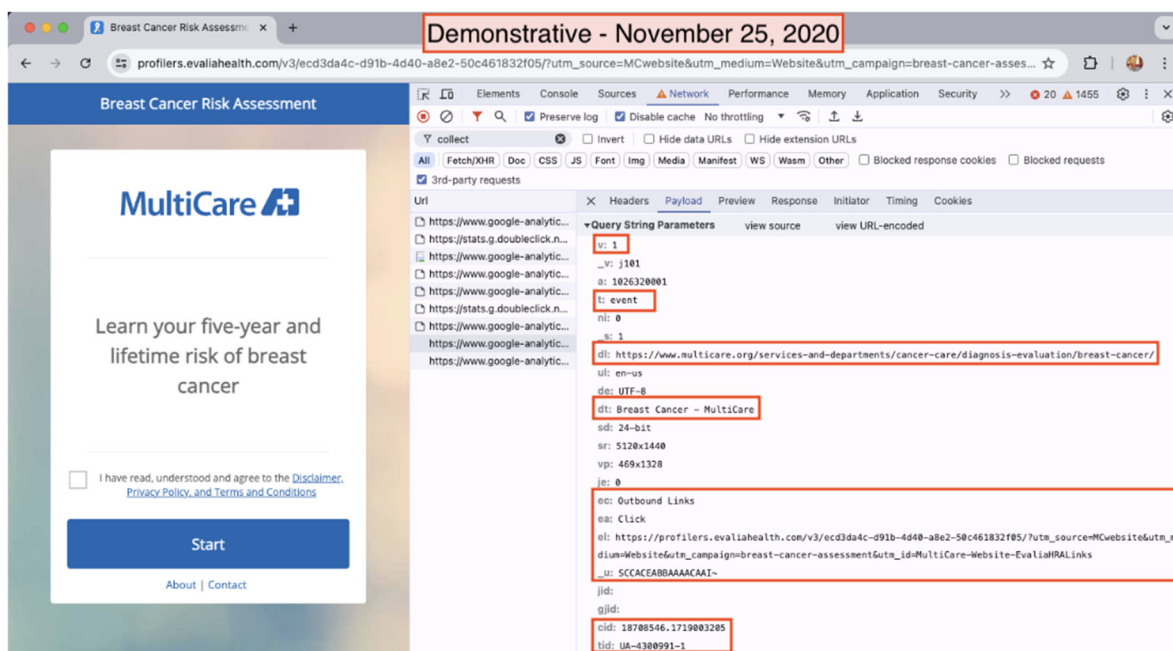
190. If the user conducted a keyword search on MultiCare's website, MultiCare would inform Google via a Click event that the user was using the search function, and a Pageview event that revealed the user's exact search terms (e.g., "search=cancer"):



191. Then, as the user clicked through their search results, MultiCare would also report those activities to Google. If the user clicked to view MultiCare’s Cancer Care and Breast Cancer pages, for example, MultiCare would transmit pageview events to Google informing it that the user navigated to pages about “services-and-department/cancer-care” and/or “diagnosis-evaluation/breast-cancer/” (see example below):



192. Furthermore, MultiCare would report users' activities within the pages that they opened from their search results too. For instance, when the user clicked to launch a breast cancer risk assessment from the Breast Cancer page, MultiCare would report that to Google through Outbound Links and Click events:



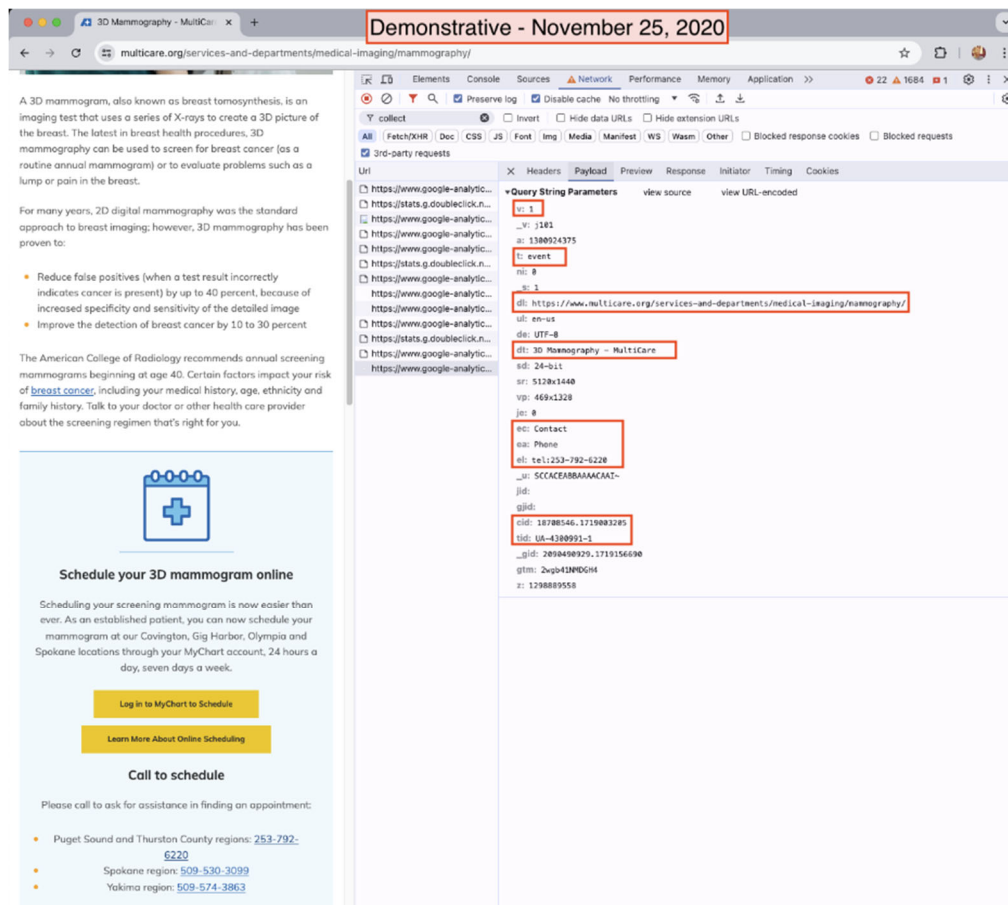


1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11

12  
13  
14  
15  
16

193. Similarly, when the user navigated to the 3D Mammography page and then called MultiCare to schedule an appointment, MultiCare would disclose that as well through pageview and Phone events, with the Phone event disclosing that the user clicked to call MultiCare while they were on the “3D Mammography – Multicare” page:

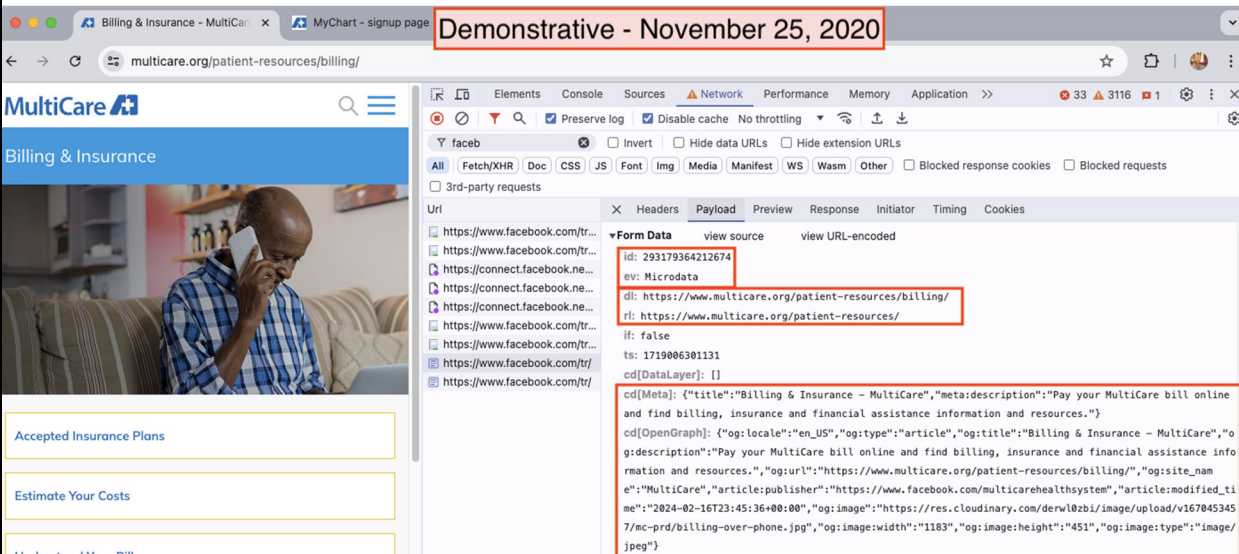
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27



## 9. MultiCare Disclosed Users' Patient Portal Activities & Bill Pay Activities to Meta and Google

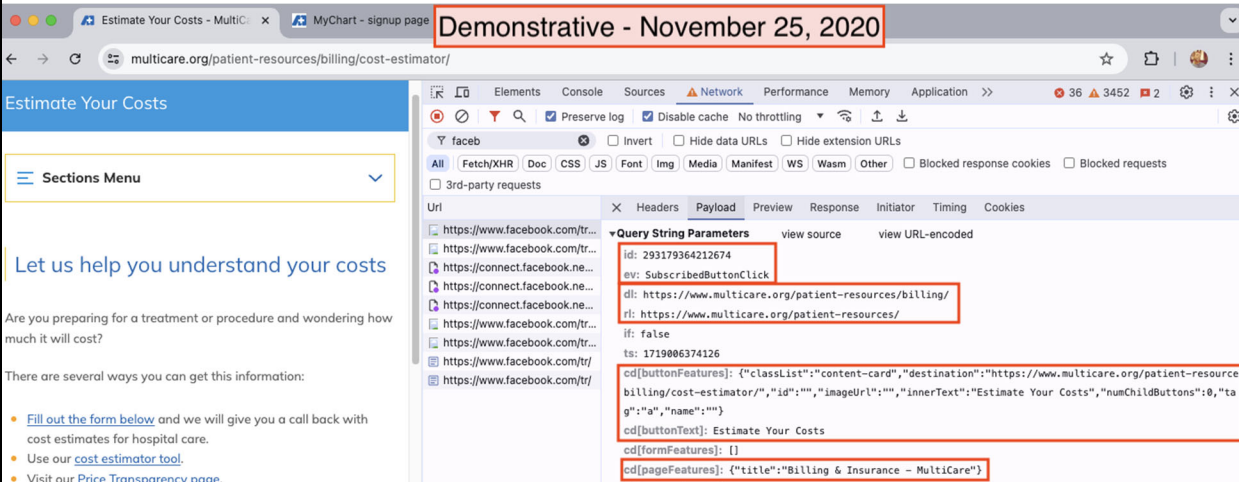
194. Upon the User's navigation to MultiCare's Billing & Insurance page, MultiCare would send SubscribedButtonClick, PageView, and Microdata events to Facebook disclosing their patient status and patient activities (see examples below).





195. From the Billing & Insurance page, the User could perform a variety of activities including obtaining cost estimates and paying their medical bills. MultiCare informed Facebook when the User performed each of these activities.

196. For example, when the User clicked to obtain estimates, MultiCare would send a SubscribedButtonClick event, revealing that the User clicked on a button labeled “Estimate Your Costs,” while they were on a page for “Billing & Insurance - MultiCare”:



197. When the next page loaded, MultiCare would then send User data via PageView and Microdata events, confirming that the User was on the page for “billing/cost-estimator/” where the User could obtain cost estimates as they prepared for medical treatments or procedures (see example below):

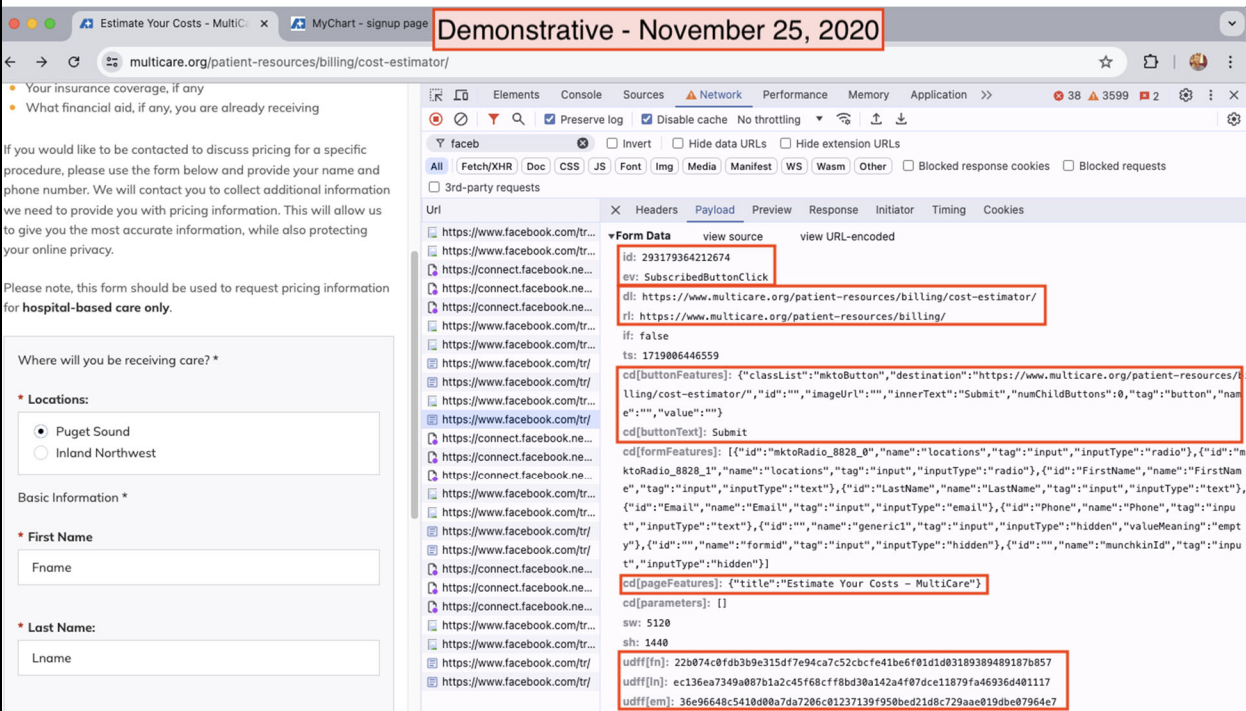
Query String Parameters    view source    view URL-encoded

```

id: 293179364212674
ev: SubscribedButtonClick
dl: https://www.multicare.org/patient-resources/billing/
rl: https://www.multicare.org/patient-resources/
if: false
ts: 1719006374126
cd[buttonFeatures]: {"classList":"content-card","destination":"https://www.multicare.org/patient-resources/billing/cost-estimator/","id":"","imageUrl":"","innerText":"Estimate Your Costs","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]: Estimate Your Costs
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Billing & Insurance - MultiCare"}

```

198. Once on the estimates page, the User could request pricing information by inputting their information. As the User clicked to submit their information, MultiCare would send a SubscribedButtonClick event, not only indicating that the User clicked “Submit” while they were on the “Estimate Your Costs – MultiCare” page, but also disclosing to Facebook the first/last name and email address of the User filling out the form, as evidenced by the “udff” parameters in the example below:

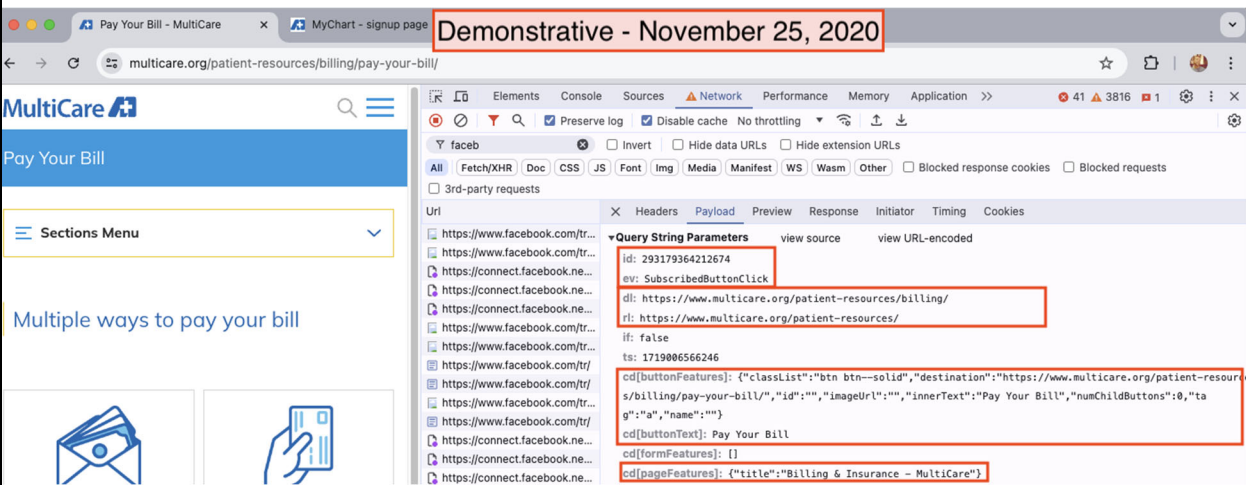


199. The fact that the SubscribedButtonClick event transmitted to Facebook hashed “udf” values from the forms filled out by the Users means that MultiCare enabled the “Advanced Matching Parameters” for the Meta Pixel, which allows Meta to connect collected event data to users, even if they do not have Facebook’s browser cookie activated (the c\_user cookie which serves as a unique personal identifier to Meta).

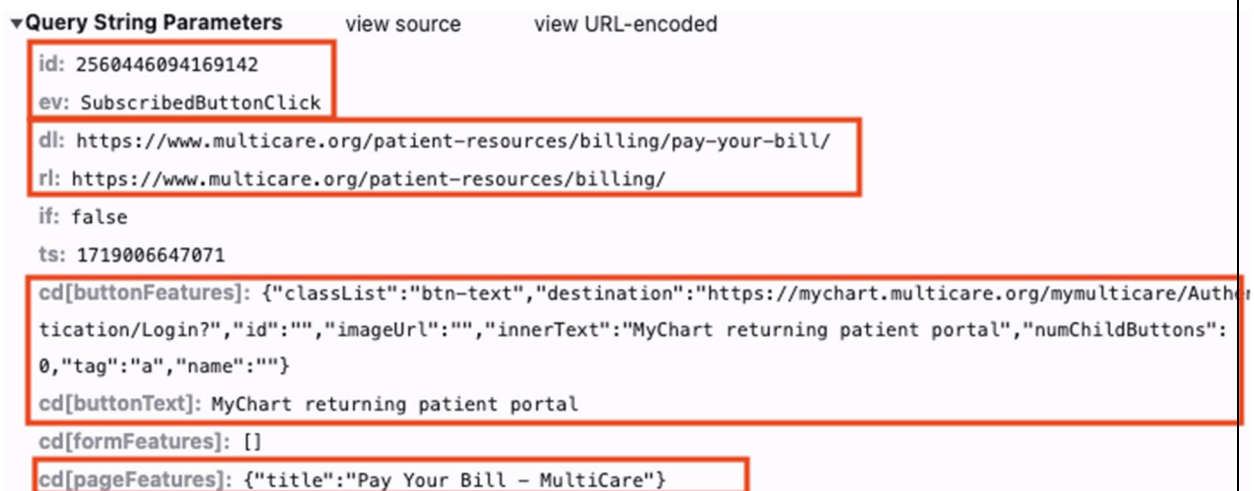
200. In other words, MultiCare enabled its Pixels to capture and disclose to Facebook additional personal identifiers such as the Users’ names, emails and phone numbers – all of which are used by Facebook to link collected data to individual persons and create Custom Audiences for targeted advertising.<sup>62</sup>

201. In addition, MultiCare would also inform Facebook when users used the Billing & Insurance page to pay their medical bills, disclosing that the User clicked a button labeled “Pay Your Bill”:

<sup>62</sup> See <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>.

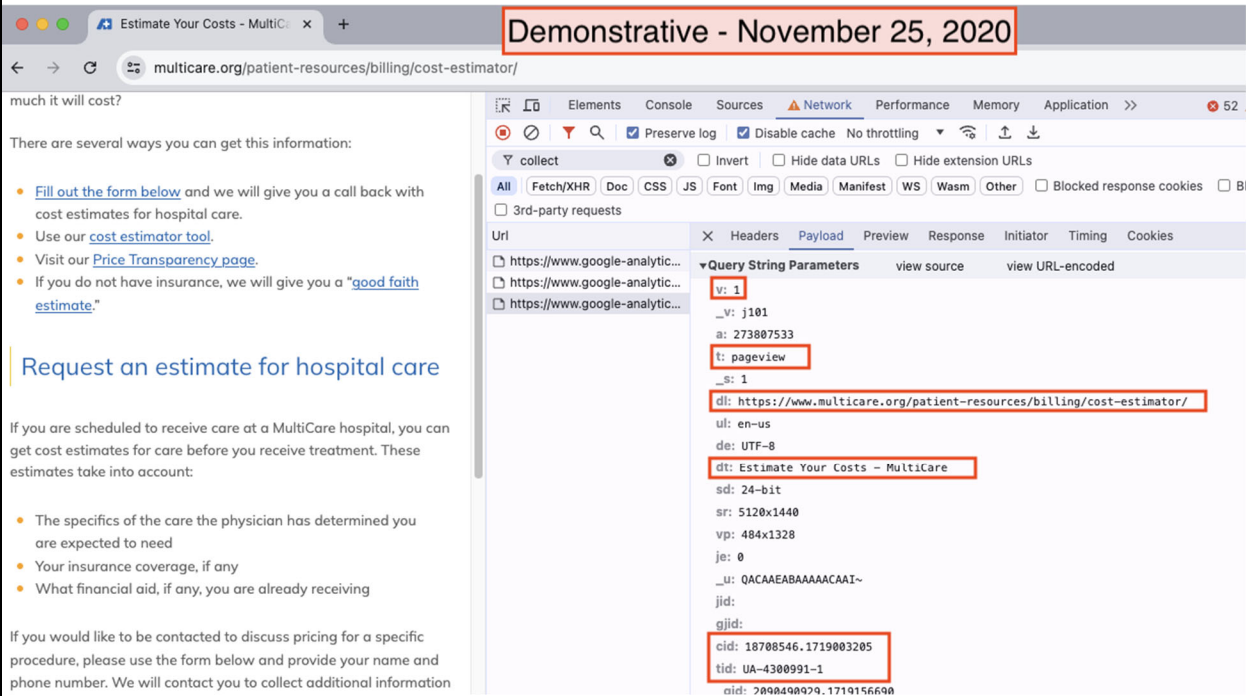


202. From the Pay Your Bill page, users have the option of paying via (i) a MyChart guest portal, (ii) by logging into their MyChart account, (iii) telephone, or (iv) mail. As a user clicked to pay or to learn more about each of these options, MultiCare would send a SubscribedButtonClick event informing Facebook whether the user clicked (i) for the “MyChart guest portal,” (ii) for the “MyChart returning patient portal,” (iii) to “Call” “tel:8009191936,” and (iv) to “Pay by mail,” while the user was on the page for “Pay Your Bill – MultiCare” (see example below):



203. MultiCare also disclosed information about Users' billing related activities to Google, via a series of Pageview events.

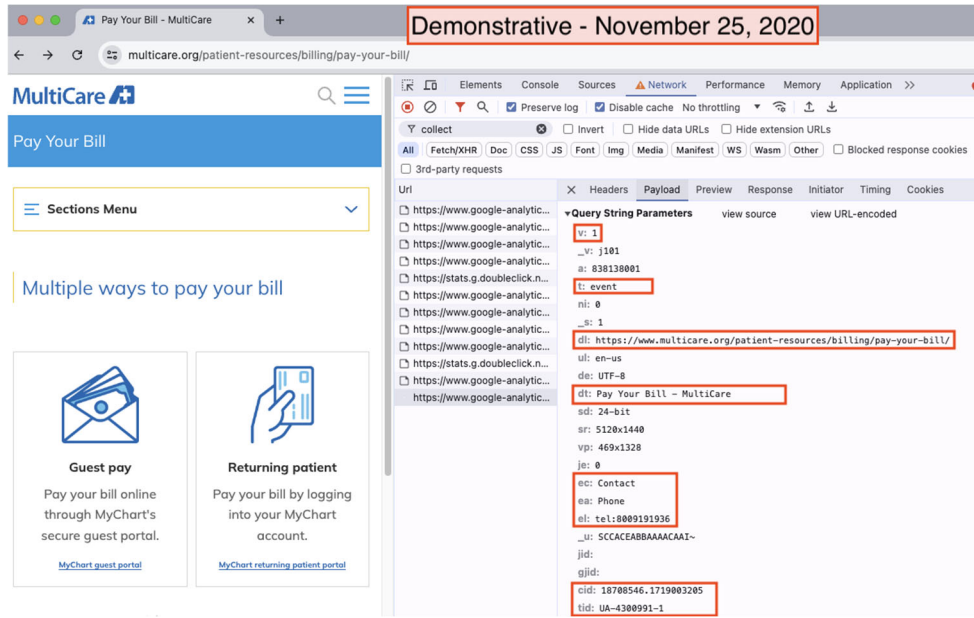
204. For example, once the User loaded for information to estimate their medical costs, MultiCare would send a Pageview event reporting that the User was viewing a page with a "cost-estimator/."



205. If the User then successfully submitted their information to request a cost estimate, MultiCare would send another Pageview event, informing Google that the user was on a page named "Thank You – MultiCare."

206. Additionally, MultiCare also disclosed when Users navigate to pay their medical bills. When the User clicks to call MultiCare to pay their bill, MultiCare sends a Phone event, informing Google that the User clicked to call MultiCare while they were on a page called "Pay Your Bill – MultiCare."





207. Similarly, when the user navigated to the page with additional contact information for billing related questions, MultiCare would send another pageview event, which reveals the user navigated to the page, “Billing Contact Information – MultiCare.”

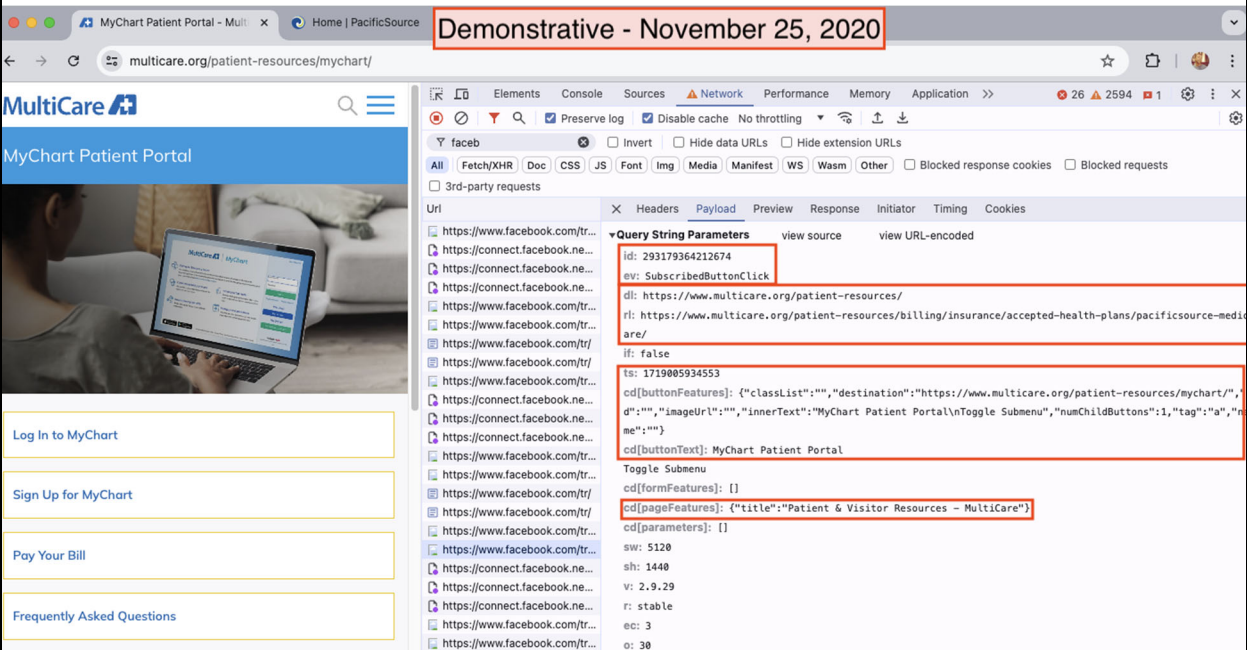
#### 10. **MultiCare Likely Installed Third-Party Tracking Software Inside its Patient Portal**

208. Given that MultiCare has been tracking patients’ activities even on the log-in pages for its Patient Portal and ‘Pay Your Bill’ pages, it is highly likely that MultiCare installed Meta and Google trackers inside its Patient Portal as well.

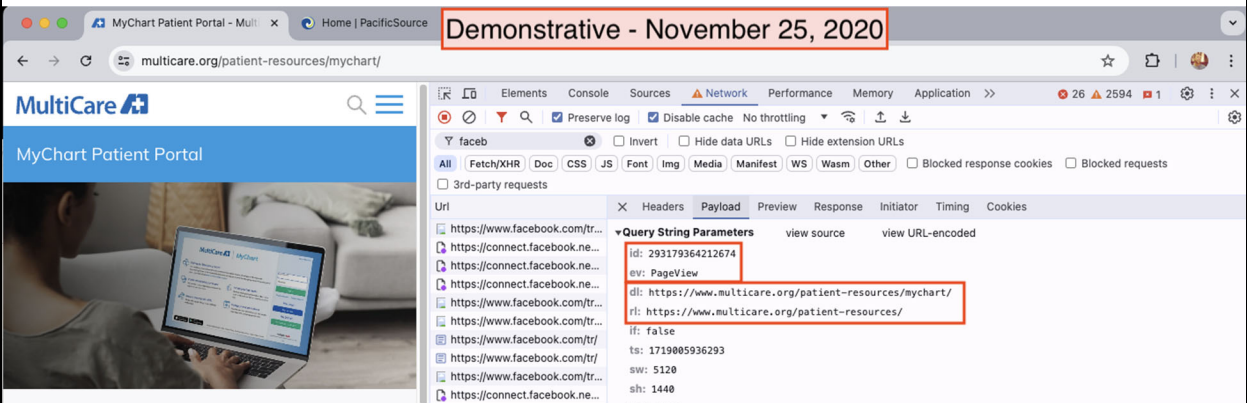
209. Discovery is needed to establish what specific tracking software MultiCare installed inside the patient portal and what information MultiCare was sharing with unauthorized third parties.

210. For example, on MultiCare’s MyChart page, Users navigate to log in, create an account, pay their bills, or learn about obtaining medical records. MultiCare informed Facebook and Google about each of these Users’ MyChart related activities.

211. As a User clicks to access MultiCare's MyChart, MultiCare sends a SubscribedButtonClick event to Facebook, informing it that the User clicked on a button for the "MyChart Patient Portal."

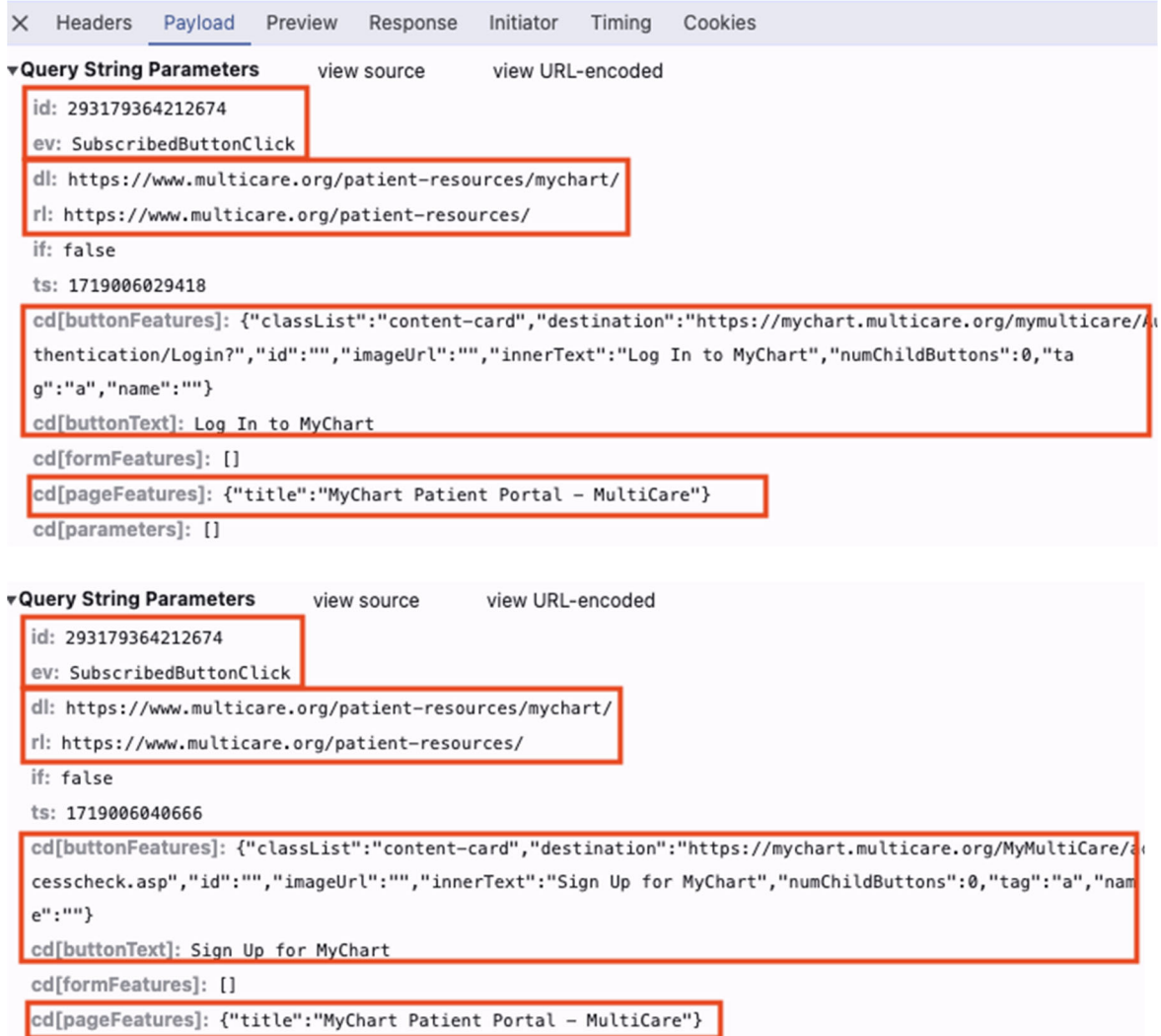


212. Once the MyChart Patient Portal page loaded, MultiCare then sent PageView and Microdata events confirming that the User loaded the page.



213. From MultiCare's MyChart Patient Portal page, Users click to log into MyChart or sign up for MyChart. As a User clicks either button, MultiCare informs Facebook of the User's actions through a SubscribedButtonClick event:





214. MultiCare also informed Facebook when Users navigate to pay their bill from the MyChart Patient Portal page. When a User clicked to pay their bill, MultiCare sent Facebook a SubscribedButtonClick event which reveals that the User clicked to “Pay Your bill,” while they were on the MyChart Patient – MultiCare page:

▼Query String Parameters view source view URL-encoded

```

id: 293179364212674
ev: SubscribedButtonClick
dl: https://www.multicare.org/patient-resources/mychart/
rl: https://www.multicare.org/patient-resources/
if: false
ts: 1719006061424
cd[buttonFeatures]: {"classList":"content-card","destination":"https://www.multicare.org/patient-resources/billing/pay-your-bill/","id":"","imageUrl":"","innerText":"Pay Your Bill","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]: Pay Your Bill
cd[formFeatures]: []
cd[pageFeatures]: {"title":"MyChart Patient Portal – MultiCare"}
cd[parameters]: {}

```

215. Users can also learn about how to schedule appointments online through the MyChart Patient Portal page. When a User does so, MultiCare sends a SubscribedButtonClick event divulging that the User clicked to learn “How to Schedule Online”:

Online Scheduling - MultiCare x MyChart - signup page Demonstrative - November 25, 2020

multicare.org/patient-resources/online-scheduling/

MultiCare

Online Scheduling

Scheduling your appointments just got easier

Book Your Appointment Online

How to schedule online

You can now schedule many primary care appointments online in two ways:

▼Query String Parameters view source view URL-encoded

```

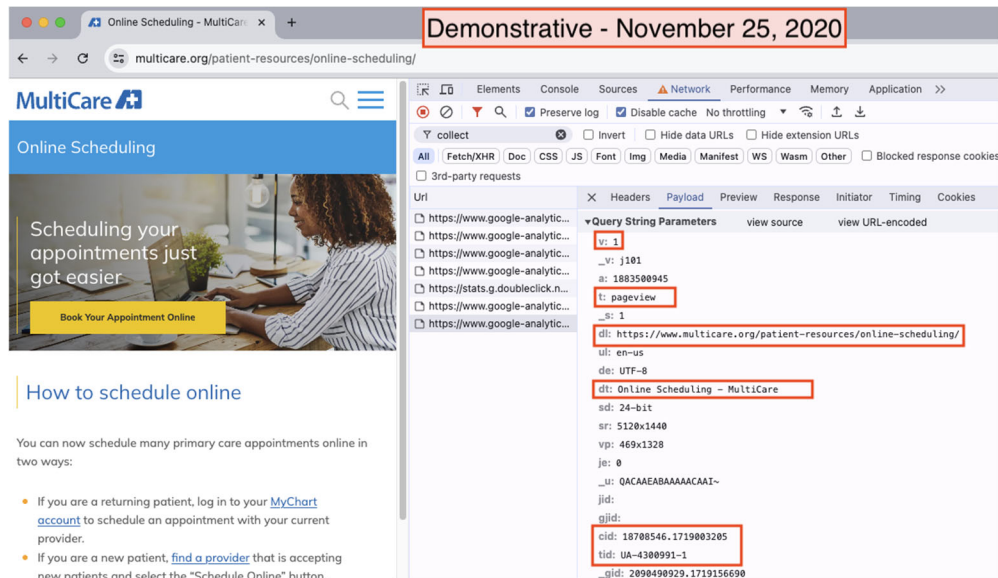
id: 293179364212674
ev: SubscribedButtonClick
dl: https://www.multicare.org/patient-resources/mychart/
rl: https://www.multicare.org/patient-resources/
if: false
ts: 1719006203721
cd[buttonFeatures]: {"classList":"btn-text","destination":"https://www.multicare.org/patient-resources/online-scheduling/","id":"","imageUrl":"","innerText":"How to Schedule Online","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]: How to Schedule Online
cd[formFeatures]: []
cd[pageFeatures]: {"title":"MyChart Patient Portal – MultiCare"}
cd[parameters]: {}

```

216. MultiCare also sends sensitive personal data about Users’ MyChart related activities to Google.

217. As soon as a User loads the MyChart page, MultiCare transmits a pageview event reporting that the User was on the page, “MyChart Patient Portal – MultiCare”:

218. If the User then navigates to a page to learn how to schedule medical appointments online, MultiCare then sends another pageview event which reports to Google that the User loaded the page for “patient-resources/online-scheduling”:



## 11. MultiCare's Privacy Policies & Promises.

219. MultiCare's privacy policies represent to Plaintiff and Class Members that MultiCare will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

220. MultiCare publishes several privacy policies that represent to Users that MultiCare will keep sensitive information confidential and that it will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.<sup>63</sup>

221. MultiCare's separate Notice of Privacy Practices assures Plaintiff and Class Members that "MultiCare uses reasonable data collection, storage and processing practices and security measures to protect your data."<sup>64</sup>

222. MultiCare's Notice of Privacy Practices explains MultiCare's duties with respect to IIHI and the exceptions for when MultiCare can use and disclose Plaintiff's and Class Members' PHI in the following ways:

- MultiCare may also share your information consistent with the Notice of Privacy Practices [including]:
  - Your Choices;
  - Treatment;

<sup>63</sup> See <https://www.multicare.org/about/policies-notice/website-privacy-policy/> last visited June 28, 2024).

<sup>64</sup> *Id.*

- Payment;
- Health System Operations;
- Public Health and Safety;
- Research;
- Limited Data Set Information;
- Comply with the Law;
- Organ and Tissue Donation;
- Coroners, Medical Examiners, and Funeral Directors;
- Workers' Compensation;
- Government Requests and Law Enforcement;
- Lawsuits and Disputes;
- Contacting You;
- Treatment Alternatives;
- Health-Related Benefits and Services;
- Inmates;
- Incidental Disclosures;
- Blood Conservation Services;
- Serious and imminent threats.<sup>65</sup>

223. MultiCare's privacy policy does not permit MultiCare to use and disclose Plaintiff's and Class Members' IIHI for marketing purposes. MultiCare promise patients that "All other information that is shared in a way not addressed in this notice, **including uses or disclosures for marketing purposes**, or disclosures of your information in exchange for some form of payment, will be made only after you give your written permission or as required by law."<sup>66</sup> (emphasis added)

224. Notwithstanding these representations, MultiCare installed Google Analytics and Meta's Collection Tools on its Web Properties and, thereafter, began to automatically transmit extensive IIHI from everyone who visited its Web Properties to Google and Meta.

225. After receiving IIHI communicated on MultiCare's Web Properties, Google and Meta analyze and use this information for their own commercial purposes that include building more fulsome profiles of its Users' preferences and traits and selling targeted advertisements based on this information. Google and Meta also receive an additional

---

<sup>65</sup> See <https://www.multicare.org/wp-content/uploads/2020/12/Notice-of-Privacy-Practices.pdf> (last Accessed June 28, 2024).

<sup>66</sup> *Id.*

1 commercial benefit from MultiCare's use of the Google and Meta Collection Tools, namely  
2 that it provides MultiCare with a greater incentive to advertise on Google and Meta's  
3 platforms.

4 226. After receiving IIHI communicated on MultiCare's Web Properties, Google and  
5 Meta forward this data, and its analysis of this data, to MultiCare. MultiCare then uses this  
6 data and analysis for its own commercial purposes that include understanding how Users use  
7 its Website and determining what ads Users see on its Website.

8 227. At all times relevant to this Complaint, MultiCare did not notify Users that it  
9 automatically sends IIHI communicated on its Web Properties to Google and Meta.

10 228. At all times relevant to this Complaint, MultiCare did not notify Users of its  
11 Web Properties that IIHI they communicate on its Web Properties were being used by Google  
12 and Meta for commercial purposes.

13 229. At all times relevant to this Complaint, MultiCare did not notify Users of its  
14 Web Properties that it was using the IIHI they communicate on its Web Properties for  
15 commercial purposes.

16 230. Neither Google nor Meta has secured any informed consent or written  
17 permission allowing them to use IIHI communicated on MultiCare's Web Properties for  
18 commercial purposes.

19 231. MultiCare has not secured any informed consent or written permission allowing  
20 it to share IIHI communicated on its Web Properties with Google or Meta or for commercial  
21 purposes.

22 232. MultiCare violated its own privacy policy by unlawfully intercepting and  
23 disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties  
24 without adequately disclosing that it shared Private Information with third parties and without  
25 acquiring the specific patients' consent or authorization to share the Private Information.  
26  
27

12. **MultiCare’s Conduct Violates Federal & State Privacy Laws.**

a. *The HIPAA Privacy Rule Protects Patient Healthcare Information.*

233. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by HHS.

234. The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.”<sup>67</sup>

235. The Privacy Rule broadly defines PHI as “individually identifiable health information” that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

236. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

237. Under the HIPAA de-identification rule, “health information is not individually-identifiable only if: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2)

---

<sup>67</sup> The HIPAA Privacy Rule, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (last visited Jun. 19, 2024).



1 “the following identifiers of the individual or of relatives, employers, or household members  
2 of the individual are removed:

- 3 a. Names;
- 4 b. Medical record numbers;
- 5 c. Account numbers;
- 6 d. Device identifiers and serial numbers;
- 7 e. Web Universal Resource Locators (URLs);
- 8 f. Internet Protocol (IP) address numbers; ... and
- 9 g. Any other unique identifying number, characteristic, or code...; and” the  
10 covered entity must not “have actual knowledge that the information  
11 could be used alone or in combination with other information to identify  
12 an individual who is subject of the information.” 45 C.F.R. § 164.514.

13 238. The HIPAA Privacy Rule requires any “covered entity”—which includes  
14 healthcare providers like MultiCare—to maintain appropriate safeguards to protect the privacy  
15 of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI  
16 without authorization. 45 C.F.R. §§ 160.103, 164.502.

17 239. An individual or corporation violates the HIPAA Privacy Rule if it knowingly:  
18 “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-  
19 identifiable health information relating to an individual.” The statute states that a “person ...  
20 shall be considered to have obtained or disclosed individually-identifiable health information  
21 ... if the information is maintained by a covered entity ... and the individual obtained or  
22 disclosed such information without authorization.” 42 U.S.C. § 1320(d)(6).

23 240. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply  
24 directly to MultiCare when it is knowingly disclosing IHI relating to an individual, as those  
25 terms are defined under HIPAA.



241. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where “the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains IHI relating to an individual “shall be fined not more than \$250,000, imprisoned not more than 10 years, or both.” 42 U.S.C. § 1320(d)(6)(b)(1).

*b. HIPAA Protects Patient Status Information.*

242. HIPAA also protects against revealing an individual’s status as a patient of a healthcare provider.

243. Guidance from HHS confirms that HIPAA protects patient status:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.... **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain clinic, then this information would be PHI.**<sup>68</sup>

244. HHS’s guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or disclosure of his or his protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, **covered**

<sup>68</sup> Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>.

1 **entities may not sell lists of patients to third parties without**  
 2 **obtaining authorization from each person on the list.**<sup>69</sup>

3 245. HHS has previously instructed that the HIPAA Privacy Rule protects patient  
 4 status:

- 5 a. “The sale of a patient list to a marketing firm” is not permitted  
 6 under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);  
 7 b. “A covered entity must have the individual’s prior written  
 8 authorization to use or disclose protected health information  
 9 for marketing communications,” which includes disclosure of  
 10 mere patient status through a patient list. 67 Fed. Reg. 53186  
 11 (Aug. 14, 2002);  
 12 c. It would be a HIPAA violation “if a covered entity  
 13 impermissibly disclosed a list of patient names, addresses, and  
 14 hospital identification numbers.” 78 Fed. Reg. 5642 (Jan. 25,  
 15 2013); and  
 16 d. The only exception permitting a hospital to identify patient  
 17 status without express written authorization is to “maintain a  
 18 directory of individuals in its facility” that includes name,  
 19 location, general condition, and religious affiliation when used  
 20 or disclosed to “members of the clergy” or “other persons who  
 21 ask for the individual by name.” 45 C.F.R. § 164.510(1). Even  
 22 then, patients must be provided an opportunity to object to the  
 23 disclosure of the fact that they are a patient. 45 C.F.R. §  
 24 164.510(2).

25 c. *HIPAA’s Protections Do Not Exclude Internet Marketing.*

26 246. As OCR reminded entities regulated under HIPAA (like MultiCare) in its  
 27 recently issued *Use of Online Tracking Technologies by HIPAA Covered Entities and*  
*Business Associates* bulletin:

Regulated entities are not permitted to use tracking technologies  
 in a manner that would result in impermissible disclosures of PHI  
 to tracking technology vendors or any other violations of the  
 HIPAA Rules. ***For example, disclosures of PHI to tracking***  
***technology vendors for marketing purposes, without individuals’***

<sup>69</sup> Marketing, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html>

*HIPAA-compliant authorizations, would constitute impermissible disclosures.*<sup>70</sup>

247. OCR makes it clear that information that is routinely collected by vendors on public-facing websites may be PHI including, but not limited to, unique identifiers such as IP addresses, device IDs or email addresses.<sup>71</sup>

248. Further, HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal, *i.e.*, to "unauthenticated" webpages:

[T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal ... [and *pages*] *that permit[] individuals to schedule appointments without entering credentials may have access to PHI in certain circumstances.* For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.<sup>72</sup>

249. **The HHS bulletin reminds covered entities, like MultiCare, of their long-standing duty to safeguard PHI**, explicitly noting that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," and proceeding to explain how online tracking technologies violate the same HIPAA privacy rules that have existed for decades.<sup>73</sup>

250. Disclosures of PHI for online marketing or sales purposes require patient authorization under HIPAA, which MultiCare did not obtain here. *See* 45 CFR §

<sup>70</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, (emphasis added) (updated March 18, 2024) (last visited Jun. 19, 2024).

<sup>71</sup> *See id.*

<sup>72</sup> *Id.*

<sup>73</sup> *Id.* (emphasis added).

1 164.508(a)(3) (“a covered entity must obtain an authorization for any use or disclosure of  
 2 protected health information for marketing, except if the communication is in the form of: (A)  
 3 a face-to-face communication made by a covered entity to an individual; or (B) a promotional  
 4 gift of nominal value provided by the covered entity.”); 45 CFR § 164.508(a)(4) (“a covered  
 5 entity must obtain an authorization for any disclosure of protected health information which is  
 6 a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch  
 7 authorization must state that the disclosure will result in remuneration to the covered entity.”).

8 251. As a result, a healthcare provider like MultiCare may not disclose PHI to a  
 9 tracking technology vendor, like Meta or Google, unless it has properly notified Website  
 10 Users and entered into a business associate agreement with the vendor in question.

11 252. Yet MultiCare disclosed Plaintiff’s and Class Members’ PHI without their  
 12 consent and without a business associate agreement with Meta or Google.

13 *d. Under HIPAA, IP Addresses are Personally Identifiable Information.*

14 253. Through the use of the Google and Meta Collection Tools, computer IP  
 15 addresses are among the Private Information that was improperly disclosed to Facebook.

16 254. An IP address is a number that identifies the address of a device connected to  
 17 the Internet.

18 255. IP addresses are used to identify and route communications on the Internet.

19 256. IP addresses of individual Internet users are used by Internet service providers,  
 20 websites, and third-party tracking companies to facilitate and track Internet communications.

21 257. Facebook tracks every IP address ever associated with a Facebook user.

22 258. Google also tracks IP addresses associated with Internet users.

23 259. Facebook, Google, and other third-party marketing companies track IP  
 24 addresses for use of tracking and targeting individual homes and their occupants with  
 25 advertising by using IP addresses.

26 260. Under HIPAA, an IP address is considered PII:  
 27

a. HIPAA defines PII to include “any unique identifying number, characteristic or code” and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

261. Consequently, by disclosing Plaintiff’s and Class Members’ IP addresses along with making their healthcare appointments, paying their medical bills or logging into (or using) the patient portal for their medical care, MultiCare’s business practices violated HIPAA and industry privacy standards.

*e. The FTC Act Protects Health Information.*

262. The FTC has made clear that “health information” is “anything that conveys information—or enables an information—about a consumer’s health” and provides an example that location-data alone (such as repeated trips to a cancer treatment facility”) “may convey highly sensitive information about a consumer’s health.”<sup>74</sup>

263. The FTC joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such “health information” with Google and Facebook is an unfair business practice under federal law:

When consumers visit a hospital’s website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties,” said Samuel Levine, Director of the FTC’s Bureau of Consumer Protection. “The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect

<sup>74</sup> Jillson, Elisa, *Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>.

consumers' health information from potential misuse and exploitation."<sup>75</sup>

264. While the OCR's guidance on some of these topics was vacated in part due to improper rulemaking, the *FTC's* guidance on these topics remains unchanged and its enforcement actions remain in effect and highly instructive.

*f. MultiCare Violated Industry Standards.*

265. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

266. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

267. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

268. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

269. AMA Code of Medical Ethics Opinion 3.3.2 provides:

---

<sup>75</sup> *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...(c) release patient information only in keeping ethics guidelines for confidentiality.

**13. Plaintiff's & Class Members' Expectations of Privacy.**

270. Plaintiff and Class Members were aware of MultiCare's duty of confidentiality when they sought medical services from MultiCare.

271. Indeed, at all times when Plaintiff and Class Members provided their PII and/or PHI to MultiCare, they each had a reasonable expectation that the information would remain private and that MultiCare would not share their Private Information with third parties for a commercial purpose, unrelated to patient care.

272. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

273. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.<sup>76</sup>

274. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

275. Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information are grounded in, among other things, MultiCare's status as a healthcare provider, MultiCare's common law obligation to maintain the confidentiality of patients' Private Information, state and federal laws protecting the confidentiality of medical

---

<sup>76</sup> *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), available at <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited Apr. 19, 2024).



information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and MultiCare's express and implied promises of confidentiality.

**14. Patients Have Protectable Property Interests in Their IIHI.**

276. Property is the right of any person to possess, use, enjoy or dispose of a thing, including intangible things like data and communications. Plaintiff and Class Members have a vested property right in their IIHI.

277. Federal and state laws grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

278. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

279. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA. State health privacy laws and American courts have also long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

280. Property rights in communications and information privacy are established by:

- a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act); and
- b. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, *see Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

281. Meta’s CEO, Mark Zuckerberg, has acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its “Download Your Information” tool, Zuckerberg stated that, “People own and have control over all info they put into Facebook and ‘Download Your Information’ enables people to take stuff with them.”<sup>77</sup> Although Zuckerberg’s statements regarding people’s ability to “control” the information “put into Facebook” and the ability to access all such data via DYI is not true, his statement about data ownership is true.

282. MultiCare’s unauthorized interception and disclosure of Plaintiff’s and Class Members’ IIHI violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

**15. The Information MultiCare Discloses to Google and Meta Without Plaintiff’s or Class Members’ Consent Has Actual, Measurable Monetary Value.**

283. After receiving IIHI communicated on MultiCare’s Web Properties, both Google and Meta forward their analysis of this data to MultiCare. MultiCare then uses that analysis for its own commercial purposes, including to target ads at existing patients or other people with characteristics similar to certain groups of Users.

284. Technology companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

285. Meta “generate[s] substantially all of [its] revenue from advertising.”<sup>78</sup>

286. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including Google, who are targeting Facebook users based on their health information.

<sup>77</sup> <https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/>.

<sup>78</sup> Meta 2022 Annual Report at 17.

1           287. Similarly, Google a vast majority of its revenue from advertising. Google  
2 annually receives billions of dollars of unearned advertising sales revenue from Google  
3 healthcare Partners who target Google users based on their health information.

4           288. The robust market for Internet user data has been analogized to the “oil” of the  
5 tech industry.<sup>79</sup> A 2015 article from TechCrunch accurately noted that “[d]ata has become a  
6 strategic asset that allows companies to acquire or maintain a competitive edge.”<sup>80</sup>

7           289. That article noted that the value of a single Internet user—or really, a single  
8 user’s data—varied from about \$15 to more than \$40.

9           290. Conservative estimates suggest that in 2018, Internet companies earned \$202  
10 per American user from mining and selling data (after costs).<sup>81</sup> At the time, estimates for 2022  
11 were as high as \$434 per user, for a total of more than \$200 billion industry wide.

12           291. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes:  
13 “Personal information is an important currency in the new millennium. The monetary value of  
14 personal data is large and still growing, and corporate America is moving quickly to profit  
15 from the trend. Companies view this information as a corporate asset and have invested  
16 heavily in software that facilitates the collection of consumer information.”<sup>82</sup>

17           292. This economic value has been leveraged largely by corporations who pioneered  
18 the methods of its extraction, analysis and use. However, the data also has economic value to  
19 Internet users. Market exchanges have sprung up where individual users like Plaintiff herein  
20 can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay  
21 Internet users for their data.<sup>83</sup>

22  
23 <sup>79</sup> See [https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-](https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data)  
data (last visited Apr. 19, 2024).

24 <sup>80</sup> See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last visited Jan. 9, 2024).

25 <sup>81</sup> See *What Your Data is Really Worth to Facebook* (Jul. 12, 2019),  
<https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/> (last visited Apr. 19,  
2024).

26 <sup>82</sup> Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

27 <sup>83</sup> See *10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last visited  
Jan. 9, 2024).

1           293. There are countless examples of this kind of market, which is growing more  
2 robust as information asymmetries are diminished through revelations to users as to how their  
3 data is being collected and used.

4           294. Courts recognize the value of personal information and the harm when it is  
5 disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494  
6 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination  
7 of their personal information and by losing the sales value of that information were sufficient  
8 to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc.,*  
9 *Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the  
10 value that personal identifying information has in our increasingly digital economy").

11           295. Healthcare data is particularly valuable on the black market because it often  
12 contains all of an individual's PII and medical conditions as opposed to a single piece of  
13 information that may be found in a financial breach.

14           296. Healthcare data is incredibly valuable because, unlike a stolen credit card that  
15 can be easily canceled, most people are unaware that their medical information has been sold.  
16 Once it has been detected, it can take years to undo the damage caused.

17           297. The value of health data is well-known and various reports have been conducted  
18 to identify its value.

19           298. Specifically, in 2023, the Value Examiner published a report entitled Valuing  
20 Healthcare Data. The report focused on the rise in providers, software firms and other  
21 companies that are increasingly seeking to acquire clinical patient data from healthcare  
22 organizations. The report cautioned providers that they must de-identify data and that  
23 purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate  
24 any regulatory risk."<sup>84</sup>

---

25  
26 <sup>84</sup> *See*  
27 <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf>  
(last visited Apr. 19, 2024).

299. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).<sup>85</sup>

300. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.<sup>86</sup>

301. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”<sup>87</sup>

302. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

303. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users’ stolen data, surely Internet users can sell their own data.

304. In short, there is a quantifiable economic value to Internet users’ data that is greater than zero. The exact number will be a matter for experts to determine.

**16. MultiCare was Enriched & Benefitted from the Use of The Google & Meta Collection Tools & Unauthorized Disclosures.**

305. MultiCare installed the Google and Meta Collection Tools on the Web Properties to benefit its own marketing and revenue.

<sup>85</sup> See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (last visited Jan. 9, 2024) (citing [https://www.infopoint-security.de/media/TrustwaveValue\\_of\\_Data\\_Report\\_Final\\_PDF.pdf](https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf)).

<sup>86</sup> See <https://time.com/4588104/medical-data-industry/> (last visited Apr. 19, 2024).

<sup>87</sup> See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Apr. 19, 2024).

1           306. In exchange for disclosing the PII of its patients, MultiCare is compensated by  
2 Google and Facebook in the form of enhanced advertising services and more cost-efficient  
3 marketing.

4           307. Retargeting is a form of online marketing that targets users with ads based on  
5 their previous Internet communications and interactions. In particular, retargeting operates  
6 through code and tracking pixels placed on a website and cookies to track website visitors and  
7 then places ads on other websites the visitor goes to later.<sup>88</sup>

8           308. The process of increasing conversions and retargeting occurs in the healthcare  
9 context by sending a successful action on a healthcare website back to Google and Facebook  
10 via the tracking technologies and the Google and Meta Collection Tools embedded on, in this  
11 case, MultiCare’s Web Properties. For example, when a User searches for doctors or medical  
12 conditions or treatment on MultiCare’s Web Properties, that information is sent to Facebook.  
13 Facebook can then use its data on the User to find more users to click on a MultiCare ad and  
14 ensure that those Users targeted are more likely to convert.<sup>89</sup>

15           309. Through this process, the Google and Meta Collection Tools load and captures  
16 as much data as possible when a User loads a healthcare website that has installed the Google  
17 and Meta Collection Tools. The information the Google and Meta Collection Tools capture,  
18 “includes URL names of pages visited, and actions taken—all of which could be potential  
19 examples of health information.”<sup>90</sup>

20           310. Plaintiff’s and Class Members’ Private Information has considerable value as  
21 highly monetizable data especially insofar as it allows companies to gain insight into their  
22 customers so that they can perform targeted advertising and boost their revenues.

24 <sup>88</sup> *The complex world of healthcare retargeting*, <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last visited Apr. 19, 2024).

25 <sup>89</sup> *See, e.g., How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023),  
26 <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking>  
(last visited Apr. 19, 2024).

27 <sup>90</sup> *Id.*



1           311. In exchange for disclosing the Private Information of their account holders and  
2 patients, MultiCare is compensated in the form of enhanced advertising services and more  
3 cost-efficient marketing on its platform.

4           312. But companies have started to warn about the potential HIPAA violations  
5 associated with using pixels and tracking technologies because many such trackers are not  
6 HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.<sup>91</sup>

7           313. For example, Freshpaint, a healthcare marketing vendor, cautioned that “Meta  
8 isn’t HIPAA-compliant. They don’t sign BAAs, and the Meta Pixel acts like a giant personal  
9 user data vacuum sending PHI to Meta servers,” and “[i]f you followed the Facebook (or  
10 other general) documentation to set up your ads and conversion tracking using the Meta Pixel,  
11 remove the Pixel now.”<sup>92</sup>

12           314. Meta’s Terms of Service, Data Policy, and Cookies Policy neither inform  
13 Facebook users that Meta may acquire their health information when they interact with  
14 healthcare providers’ websites and applications, nor obtain their consent for any such  
15 acquisitions.

16           315. Google’s Terms of Service, Data Policy, and Cookies Policy neither inform  
17 Google users that Google may acquire their health information when they interact with  
18 healthcare providers’ websites and applications, nor obtain their consent for any such  
19 acquisitions.

20           316. Medico Digital also warns that “retargeting requires sensitivity, logic and  
21 intricate handling. When done well, it can be a highly effective digital marketing tool. But  
22 when done badly, it could have serious consequences.”<sup>93</sup>

23  
24  
25 <sup>91</sup> See *The guide to HIPAA compliance in analytics*, [https://campaign.piwik.pro/wp-content/uploads/2023/10/The-](https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf)  
26 [guide-to-HIPAA-compliance-in-analytics.pdf](https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf) (explaining that Google Analytics 4 is not HIPAA-compliant) (last  
27 visited Jan. 9, 2024).

<sup>92</sup> *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra*, n.92.

<sup>93</sup> *The complex world of healthcare retargeting*, *supra*, n.89.

317. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the Meta Pixel's ability to track comprehensive browsing history is also relevant. *See, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).<sup>94</sup>

318. Upon information and belief, as part of its marketing campaign, MultiCare re-targeted patients and potential patients to get more patients connected to the MultiCare Patient portal.

319. By utilizing the Google and Meta Collection Tools, the cost of advertising and retargeting was reduced, thereby benefiting MultiCare.

## **V. REPRESENTATIVE PLAINTIFF EXPERIENCE**

### **A. Plaintiff Darryl Small's Experience**

320. On numerous occasions, from at least 2019 to the present, Plaintiff accessed MultiCare's Patient Portal and MultiCare's Website on his mobile device and/or computer to receive healthcare services from MultiCare and at MultiCare's direction.

321. As a condition of receiving MultiCare's services, Plaintiff disclosed and entrusted his Private Information to MultiCare.

322. Plaintiff used MultiCare's Web Properties, including MultiCare's Patient Portal, multiple times per year to, among other things, make appointments with medical specialists, exchange messages with his providers, fill out questionnaires requested by his providers, request referrals for specific health issues, refill prescriptions, update medication information, and check medical test results.

323. Plaintiff has been in a MultiCare emergency room for an infection and received shoulder surgeries at a MultiCare hospital. As part of his treatment, Plaintiff submitted

---

<sup>94</sup> *See* Facebook Shadow Profiles (February 2022), [https://www.cesifo.org/DocDL/cesifo1\\_wp9571.pdf](https://www.cesifo.org/DocDL/cesifo1_wp9571.pdf)

1 information to MultiCare's Web Properties about each of these medical conditions. For  
2 example, in June 2024, Plaintiff exchanged messages on MultiCare's Web Properties about  
3 receiving prescription refills for various medications.

4 324. Plaintiff has also used MultiCare's Web Properties to pay medical bills.

5 325. Plaintiff has used and continues to use the same devices to maintain and access  
6 both an active Google account and an active Facebook account throughout the relevant period  
7 in this case.

8 326. Plaintiff read MultiCare's Notice of Privacy Practices concerning the  
9 circumstances under which MultiCare would share his health information when he first  
10 became a patient of MultiCare and each time he visited the policy was presented for him to  
11 read and sign.

12 327. Plaintiff provided his Private Information to MultiCare and trusted that the  
13 information would be safeguarded according to MultiCare's policies and state and federal law.

14 328. Plaintiff reasonably expected that his communications with MultiCare via the  
15 Web Properties were confidential, solely between himself and MultiCare, and that such  
16 communications would not be transmitted to or intercepted by a third party.

17 329. Pursuant to the systematic process described herein, MultiCare assisted Google  
18 and Meta with intercepting Plaintiff's communications, including those that contained PII,  
19 PHI and related confidential information.

20 330. MultiCare transmitted to Google and Meta Plaintiff's Facebook ID and/or  
21 Google 'cid' parameter cookie, IP address, other unique personal identifiers including Meta  
22 and Google cookies, and information relating to his medical conditions, including test results.

23 331. MultiCare assisted these interceptions without Plaintiff's knowledge, consent,  
24 or express written authorization. By failing to receive the requisite consent, MultiCare  
25 breached confidentiality and unlawfully disclosed Plaintiff's PII and/or PHI.  
26  
27

332. MultiCare did not inform Plaintiff that it had shared his Private Information with Google and Meta.

333. After Plaintiff disclosed his Private Information to MultiCare, he began to receive targeted ads related to his PHI, including ads about shoulder replacement services, pain relieving and anti-inflammatory medications, and certain medical tests.

334. Plaintiff suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

335. Plaintiff is an active patient of MultiCare and seeks to continue to use the Web Properties to view his test results and communicate other Private Information concerning his medical conditions with MultiCare, but fears that without court action, his Private Information will be shared with unauthorized third parties, such as Google and Meta, in the future.

336. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in MultiCare's possession, is protected and safeguarded from future unauthorized disclosure.

## VI. TOLLING

337. Any applicable statutes of limitation have been tolled by MultiCare's knowing and active concealment of its incorporation of the Google and Meta Collection Tools into its Web Properties.

338. The Google trackers Meta Pixels and other tracking tools on MultiCare's Web Properties were and are entirely invisible to a Web Properties visitor.

339. Through no fault or lack of diligence, Plaintiff and Class Members were deceived and could not reasonably discover MultiCare's deception and unlawful conduct.

1           340. Plaintiff was ignorant of the information essential to pursue his claims, without  
2 any fault or lack of diligence on his part.

3           341. MultiCare had exclusive knowledge that its Web Properties incorporated the  
4 Google trackers, Meta Pixels and other tracking tools and yet failed to disclose to its patients,  
5 including Plaintiff and Class Members, that by seeking medical care through MultiCare's  
6 Website, Plaintiff's and Class Members' Private Information would be disclosed or released  
7 to Google, Facebook, and other unauthorized third parties.

8           342. Under the circumstances, MultiCare was under a duty to disclose the nature,  
9 significance, and consequences of its collection and treatment of its patients' Private  
10 Information. In fact, to the present, MultiCare has not conceded, acknowledged, or otherwise  
11 indicated to its patients that it has disclosed or released their Private Information to  
12 unauthorized third parties. Accordingly, MultiCare is estopped from relying on any statute of  
13 limitations.

14           343. Moreover, all applicable statutes of limitation have also been tolled pursuant to  
15 the discovery rule.

16           344. The earliest that Plaintiff or Class Members, acting with due diligence, could  
17 have reasonably discovered MultiCare's conduct would have been shortly before the filing of  
18 this suit.

## 19                                   **VII. CLASS ACTION ALLEGATIONS**

20           345. Plaintiff brings this action individually and on behalf of all other persons  
21 similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

22           346. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

23                   All persons residing in the United States whose Private  
24 Information was disclosed to a third party without authorization or  
25 consent through the Google Collection Tools and/or the Meta  
26 Collection Tools on MultiCare's Web Properties.  
27

1           347. The Washington Subclass that Plaintiff seeks to represent is defined as:

2                   All persons residing in Washington whose Private Information  
3                   was disclosed to a third party without authorization or consent  
4                   through the Google Collection Tools and/or the Meta Collection  
5                   Tools on MultiCare's Web Properties.

6           348. Excluded from the Class are MultiCare, its agents, affiliates, parents,  
7           subsidiaries, any entity in which MultiCare has a controlling interest, any MultiCare officer or  
8           director, any successor or assign, and any Judge who adjudicates this case, including their  
9           staff and immediate family.

10          349. Plaintiff reserves the right to modify or amend the definition of the proposed  
11          class before the Court determines whether certification is appropriate.

12          350. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The Class Members are so numerous  
13          that joinder of all members is impracticable. Upon information and belief, there are millions  
14          of individuals whose PII and PHI may have been improperly accessed by Google and  
15          Facebook, and the Class is identifiable within MultiCare's records.

16          351. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact  
17          common to the Class exist and predominate over any questions affecting only individual Class  
18          Members. These include:

19                  a.       Whether and to what extent MultiCare had a duty to protect the Private  
20                  Information of Plaintiff and Class Members;

21                  b.       Whether MultiCare had duties not to disclose the Private Information of  
22                  Plaintiff and Class Members to unauthorized third parties;

23                  c.       Whether MultiCare violated its Privacy Policies by disclosing the  
24                  Private Information of Plaintiff and Class Members to Facebook, Google, and/or additional  
25                  third parties;

26                  d.       Whether MultiCare adequately, promptly and accurately informed  
27                  Plaintiff and Class Members that their Private Information would be disclosed to third parties;



e. Whether MultiCare violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

f. Whether MultiCare adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether MultiCare engaged in unfair, unlawful or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

h. Whether MultiCare violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of MultiCare's wrongful conduct;

j. Whether MultiCare knowingly made false representations as to its data security and/or Privacy Policy practices;

k. Whether MultiCare knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of MultiCare's disclosure of their Private Information.

352. **Typicality**, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of MultiCare's incorporation of the Google and Meta Collection Tools, due to MultiCare's misfeasance.

353. **Predominance**. MultiCare engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully disclosed in the same way. The common issues arising from MultiCare's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has

important and desirable advantages of judicial economy. MultiCare's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on MultiCare's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

354. **Adequacy of Representation**, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

355. **Superiority and Manageability**, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like MultiCare. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

356. **Policies Generally Applicable to the Class**. This class action is also appropriate for certification because MultiCare acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief

1 appropriate with respect to the Class as a whole. MultiCare's policies challenged herein apply  
2 to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on  
3 MultiCare's conduct with respect to the Class as a whole, not on facts or law applicable only  
4 to Plaintiff.

5 357. The nature of this action and the nature of laws available to Plaintiff and Class  
6 Members makes the use of the class action device a particularly efficient and appropriate  
7 procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because  
8 MultiCare would necessarily gain an unconscionable advantage since it would be able to  
9 exploit and overwhelm the limited resources of each individual Class Member with superior  
10 financial and legal resources; the costs of individual suits could unreasonably consume the  
11 amounts that would be recovered; proof of a common course of conduct to which Plaintiff  
12 was exposed is representative of that experienced by the Class and will establish the right of  
13 each Class Member to recover on the cause of action alleged; and individual actions would  
14 create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

15 358. The litigation of the claims brought herein is manageable. MultiCare's uniform  
16 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of  
17 Class Members demonstrate that there would be no significant manageability problems with  
18 prosecuting this lawsuit as a class action.

19 359. Adequate notice can be given to Class Members directly using information  
20 maintained in MultiCare's records.

21 360. Unless a Class-wide injunction is issued, MultiCare may continue in its failure  
22 to properly secure the Private Information of Class Members, MultiCare may continue to  
23 refuse to provide proper notification to Class Members regarding the practices complained of  
24 herein, and MultiCare may continue to act unlawfully as set forth in this Complaint.

25 361. Further, MultiCare acted or refused to act on grounds generally applicable to the  
26 Class and, accordingly, final injunctive or corresponding declaratory relief with regard to  
27

1 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil  
2 Procedure.

3 362. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for  
4 certification because such claims present only particular, common issues, the resolution of  
5 which would advance the disposition of this matter and the parties' interests therein. Such  
6 particular issues include, but are not limited to:

7 a. Whether MultiCare owed a legal duty to not disclose Plaintiff's and  
8 Class Members' Private Information;

9 b. Whether MultiCare owed a legal duty to not disclose Plaintiff's and  
10 Class Members' Private Information with respect to MultiCare's privacy policy;

11 c. Whether MultiCare breached a legal duty to Plaintiff and Class  
12 Members to exercise due care in collecting, storing, using, and safeguarding their Private  
13 Information;

14 d. Whether MultiCare failed to comply with its own policies and applicable  
15 laws, regulations, and industry standards relating to data security;

16 e. Whether MultiCare adequately and accurately informed Plaintiff and  
17 Class Members that their Private Information would be disclosed to third parties;

18 f. Whether MultiCare failed to implement and maintain reasonable  
19 security procedures and practices appropriate to the nature and scope of the information  
20 disclosed to third parties;

21 g. Whether Class Members are entitled to actual, consequential, and/or  
22 nominal damages, and/or injunctive relief as a result of MultiCare's wrongful conduct.

## VIII. CAUSES OF ACTION

### COUNT ONE

#### Violation of the Electronic Communications Privacy Act

18 U.S.C. § 2511(1), *et seq.*

#### Unauthorized Interception, Use and Disclosure

**(On Behalf of Plaintiff & the Nationwide Class)**

363. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

364. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

365. The ECPA protects both sending and receipt of communications.

366. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

367. The transmissions of Plaintiff's PII and PHI to MultiCare's Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

368. **Electronic Communications.** The transmission of PII and PHI between Plaintiff and Class Members and MultiCare's Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

369. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

370. MultiCare's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments.

1           371. Furthermore, MultiCare intercepted the “contents” of Plaintiff’s  
2 communications in at least the following forms:

- 3           a. The parties to the communications;
- 4           b. The precise text of patient search queries;
- 5           c. PII such as patients’ IP addresses, Facebook IDs, cid parameter cookie,  
6 browser fingerprints, and other unique identifiers;
- 7           d. The precise text of patient communications about specific doctors;
- 8           e. The precise text of patient communications about specific medical  
9 conditions;
- 10          f. The precise text of information generated when patients requested or  
11 made appointments,
- 12          g. The precise text of patient communications about specific treatments;
- 13          h. The precise text of patient communications about scheduling  
14 appointments with medical providers;
- 15          i. The precise text of patient communications about billing and payment;
- 16          j. The precise text of specific buttons on MultiCare’s Website that patients  
17 click to exchange communications including Log-Ins, Registrations,  
18 Requests for Appointments, Search, and other buttons;
- 19          k. The precise dates and times when patients click to Log-In on  
20 MultiCare’s Web Properties;
- 21          l. The precise dates and times when patients visit MultiCare’s Web  
22 Properties;
- 23          m. Information that is a general summary or informs third parties of the  
24 general subject of communications that MultiCare sends back to patients  
25 in response to search queries and requests for information about specific  
26 doctors, conditions, treatments, billing, payment, and other information.
- 27



372. For example, MultiCare’s interception of the fact that a patient views a webpage like:

<https://www.multicare.org/location/gig-harbor-medical-park/multicare-regional-cancer-center-gig-harbor/>

involves “content,” because it communicates that patient’s request for the information on that page.

373. **Interception.** The ECPA defines the interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

374. **Electronical, Mechanical or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies MultiCare, Google, and Meta use to track Plaintiff’s and the Class Members’ communications;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ computing devices
- d. MultiCare’s web servers and
- e. The Google and Meta Collection Tools, including the Meta Pixel and Google tracking code deployed by MultiCare to effectuate the sending and acquisition of patient communications.

375. By utilizing and embedding the Meta Pixel and Google tracking code on its Web Properties, MultiCare intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

1           376. Specifically, MultiCare intercepted Plaintiff's and Class Members' electronic  
2 communications via the Meta Pixel and Google tracking code, which tracked, stored, and  
3 unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such  
4 as Facebook and Google.

5           377. MultiCare's intercepted communications include, but are not limited to,  
6 communications to/from Plaintiff and Class Members regarding PII and PHI, treatment,  
7 medication, and scheduling.

8           378. This information was, in turn, used by third parties, such as Facebook and  
9 Google to 1) place Plaintiff and Class Members in specific health-related categories and 2)  
10 target Plaintiff and Class Members with advertising associated with their specific health  
11 conditions.

12           379. By intentionally disclosing or endeavoring to disclose the electronic  
13 communications of Plaintiff and Class Members to affiliates and other third parties, while  
14 knowing or having reason to know that the information was obtained through the interception  
15 of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), MultiCare violated 18  
16 U.S.C. § 2511(1)(c).

17           380. By intentionally using, or endeavoring to use, the contents of the electronic  
18 communications of Plaintiff and Class Members, while knowing or having reason to know  
19 that the information was obtained through the interception of an electronic communication in  
20 violation of 18 U.S.C. § 2511(1)(a), MultiCare violated 18 U.S.C. § 2511(1)(d).

21           381. Unauthorized Purpose. MultiCare intentionally intercepted the contents of  
22 Plaintiff's and Class Members' electronic communications for the purpose of committing a  
23 tortious act in violation of the Constitution or laws of the United States or of any State—  
24 namely, violation of HIPAA and the causes of action described below, among others.

25           382. The ECPA provides that a "party to the communication" may liable where a  
26 "communication is intercepted for the purpose of committing any criminal or tortious act in  
27

1 violation of the Constitution or laws of the United States or of any State.” 18 U.S.C §  
2 2511(2)(d).

3 383. MultiCare is not a party for purposes to the communication based on its  
4 unauthorized duplication and transmission of communications with Plaintiff and the  
5 Class. However, even assuming MultiCare is a party, MultiCare’s simultaneous, unknown  
6 duplication, forwarding, and interception of Plaintiff’s and Class Members’ Private  
7 Information does not qualify for the party exemption.

8 384. Here, as alleged above, MultiCare violated a provision of HIPAA, specifically  
9 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly  
10 disclosing IIHI to a third party.

11 385. HIPAA defines IIHI as:

12 any information, including demographic information collected  
13 from an individual, that—(A) is created or received by a health  
14 care provider ... (B) relates to the past, present, or future physical  
15 or mental health or condition of an individual, the provision of  
16 health care to an individual, or the past, present, or future payment  
17 for the provision of health care to an individual, and (i) identifies  
the individual; or (ii) with respect to which there is a reasonable  
basis to believe that the information can be used to identify the  
individual.

18 386. Plaintiff’s and Class Members’ information that MultiCare disclosed to third  
19 parties qualifies as IIHI, and MultiCare violated Plaintiff’s expectations of privacy, and  
20 constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6).  
21 MultiCare intentionally used the wire or electronic communications to intercept Plaintiff’s  
22 Private Information in violation of the law.

23 387. MultiCare’s conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused  
24 to be used cookie identifiers associated with specific patients without patient authorization;  
25 and disclosed individually identifiable health information to Facebook and/or Google without  
26 patient authorization.  
27

1           388. The penalty for violation is enhanced where “the offense is committed with  
2 intent to sell, transfer, or use individually identifiable health information for commercial  
3 advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

4           389. MultiCare’s conduct would be subject to the enhanced provisions of 42 U.S.C. §  
5 1320d-6 because MultiCare’s use of the Facebook source code was for MultiCare’s  
6 commercial advantage to increase revenue from existing patients and gain new patients.

7           390. MultiCare’s acquisition of patient communications that were used and disclosed  
8 to Facebook and Google was also done for purposes of committing criminal and tortious acts  
9 in violation of the laws of the United States and individual States nationwide as set forth  
10 herein, including:

- 11           a. Negligence;
- 12           b. Breach of express contract;
- 13           c. Breach of implied contract and
- 14           d. Breach of fiduciary duty.

15           391. MultiCare is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on  
16 the ground that it was a participant in Plaintiff’s and Class Members’ communications about  
17 their Private Information on the Web Properties, because it used its participation in these  
18 communications to improperly share Plaintiff’s and Class Members’ Private Information with  
19 Facebook and third-parties that did not participate in these communications, that Plaintiff and  
20 Class Members did not know was receiving their information, and that Plaintiff and Class  
21 Members did not consent to receive this information.

22           392. Here, as alleged above, MultiCare violated a provision of HIPAA, specifically  
23 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly  
24 disclosing individually identifiable health information to a third party.

25           393. As such, MultiCare cannot viably claim any exception to ECPA liability.

26

27

1           394. Plaintiff and Class Members have suffered damages as a direct and proximate  
2 result of MultiCare's invasion of privacy in that:

- 3           a. Learning that MultiCare has intruded upon, intercepted, transmitted,  
4 shared, and used their PII and PHI (including information about their  
5 medical symptoms, conditions, and concerns, medical appointments,  
6 healthcare providers and locations, medications and treatments, and  
7 health insurance and medical bills) for commercial purposes has caused  
8 Plaintiff and the Class Members to suffer emotional distress;
- 9           b. MultiCare received substantial financial benefits from its use of  
10 Plaintiff's and the Class Members' PII and PHI without providing any  
11 value or benefit to Plaintiff or the Class members;
- 12           c. MultiCare received substantial, quantifiable value from its use of  
13 Plaintiff's and the Class Members' PII and PHI, such as understanding  
14 how people use their Web Properties and determining what ads people  
15 see on the Web Properties, without providing any value or benefit to  
16 Plaintiff or the Class Members;
- 17           d. MultiCare failed to provide Plaintiff and the Class Members with the full  
18 value of the medical services for which they paid, which included a duty  
19 to maintain the confidentiality of patient information and
- 20           e. The diminution in value of Plaintiff's and Class Members' PII and PHI  
21 and the loss of privacy due to MultiCare making sensitive and  
22 confidential information, such as patient status, medical treatment, and  
23 appointments that Plaintiff and Class Members intended to remain  
24 private no longer private.
- 25  
26  
27

1           395. MultiCare intentionally used the wire or electronic communications to increase  
2 revenue. MultiCare specifically used the Meta Pixel and Google tracking code to track and  
3 utilize Plaintiff's and Class Members' Private Information for financial gain.

4           396. MultiCare was not acting under color of law to intercept Plaintiff's and the  
5 Class Members' wire or electronic communication.

6           397. Plaintiff and Class Members did not authorize MultiCare to acquire the content  
7 of their communications for purposes of invading their privacy via the Meta Pixel or Google  
8 tracking code.

9           398. Any purported consent that MultiCare received from Plaintiff and Class  
10 Members was not valid.

11           399. Consumers have the right to rely upon the promises that companies make to  
12 them. MultiCare accomplished the tracking and retargeting through deceit and disregard, such  
13 that an actionable claim may be made, in that it was accomplished through source code that  
14 caused third-party Pixels, tracking codes and cookies (including but not limited to the fbp, ga  
15 and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class  
16 members' computing devices as "first-party" cookies that are not blocked.

17           400. MultiCare's scheme or artifice to defraud in this action consists of:

- 18           a. the false and misleading statements and omissions in its privacy policy
- 19           set forth above, including the statements and omissions recited in the
- 20           claims below; and
- 21           b. the placement of the 'fbp' cookie on patient computing devices
- 22           disguised as a first-party cookie on MultiCare's Website rather than a
- 23           third-party cookie from Facebook.

24           401. MultiCare acted with the intent to defraud in that it willfully invaded and took  
25 Plaintiff's and Class Members' property:



a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

402. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of MultiCare's Web Properties, MultiCare's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

403. As a result of MultiCare's violation of the ECPA, Plaintiff and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

**COUNT TWO**  
**Breach of Express Contract**  
***(On behalf of Plaintiff & the Nationwide Class)***

404. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

405. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with MultiCare for the provision of medical and health care services.

406. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with MultiCare when Plaintiff first received medical care from MultiCare.

407. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with MultiCare include MultiCare's

1 promise to protect nonpublic, Private Information given to MultiCare or that MultiCare gather  
2 on its own from disclosure.

3 408. Under these express contracts, MultiCare and/or their affiliated healthcare  
4 providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class  
5 Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain  
6 such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange,  
7 Plaintiff and Members of the Class agreed to pay money for these services, and to turn over  
8 their Private Information.

9 409. Both the provision of medical services and the protection of Plaintiff and Class  
10 Members' Private Information were material aspects of these express contracts.

11 410. The express contracts for the provision of medical services – contracts that  
12 include the contractual obligations to maintain the privacy of Plaintiff and Class Members'  
13 Private Information—are formed and embodied in multiple documents, including (among  
14 other documents) MultiCare's Privacy Notice.

15 411. At all relevant times, MultiCare expressly represented in its Privacy Notice,  
16 among other things: (i) that "We understand that information about you and your medical and  
17 behavioral health is personal. We are committed to protecting health information about you  
18 and are required under federal and state law to take steps to protect this information."<sup>95</sup>; and  
19 (ii) that "MultiCare has security measures in place to prevent the loss, misuse or alteration of  
20 information under our control. MultiCare employs strict security measures to safeguard online  
21 financial transactions through the use of current industry encryption standards."<sup>96</sup>

22 412. MultiCare's express representations, including, but not limited to, express  
23 representations found in its Privacy Notice, formed and embodied an express contractual  
24

25  
26 <sup>95</sup> <https://www.multicare.org/wp-content/uploads/2020/12/Notice-of-Privacy-Practices.pdf> (last visited June 18,  
2024).

27 <sup>96</sup> <https://www.multicare.org/about/policies-notices/website-privacy-policy/> (last visited June 18, 2024)

1 obligation requiring MultiCare to implement data security adequate to safeguard and protect  
2 the privacy of Plaintiff's and Class Members' Private Information.

3 413. Consumers of healthcare value their privacy, the privacy of their dependents,  
4 and the ability to keep their Private Information associated with obtaining healthcare private.  
5 To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry  
6 standard data security protocols to protect Private Information is fundamentally less useful  
7 and less valuable than healthcare that adheres to industry-standard data security.

8 414. Plaintiff and Class Members would not have entered into these contracts with  
9 MultiCare and/or its affiliated healthcare providers as a direct or third-party beneficiary  
10 without an understanding that their Private Information would be safeguarded and protected.

11 415. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed  
12 to and did provide their Private Information to MultiCare and/or its affiliated healthcare  
13 providers, and paid for the provided healthcare in exchange for, amongst other things, both the  
14 provision of healthcare and medical services and the protection of their Private Information.

15 416. Plaintiff and Class Members performed their obligations under the contract  
16 when they paid for their health care services and provided their Private Information.

17 417. MultiCare materially breached its contractual obligation to protect the nonpublic  
18 Private Information MultiCare gathered when it disclosed that Private Information to Meta  
19 through the Meta Collection Tools, including the Meta Pixel, and to Google through Google  
20 Analytics and related technologies embedded on the Web Properties.

21 418. MultiCare materially breached the terms of these express contracts, including,  
22 but not limited to, the terms stated in the relevant Privacy Notice. MultiCare did not maintain  
23 the privacy of Plaintiff's and Class Members' Private Information as evidenced by  
24 MultiCare's sharing of that Private Information with Google and Meta through the Google  
25 and Meta Collection Tools on the Web Properties.  
26  
27

1           419. The mass and systematic disclosure of Plaintiff's and Class Members' Private  
2 Information to third parties, including Meta and Google, was a reasonably foreseeable  
3 consequence of MultiCare's actions in breach of these contracts.

4           420. As a result of MultiCare's failure to fulfill the data privacy protections promised  
5 in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the  
6 bargain, and instead received healthcare and other services that were of a diminished value to  
7 that described in the contracts.

8           421. Plaintiff and Class Members therefore were damaged in an amount at least  
9 equal to the difference in the value of the healthcare with data privacy protection they paid for  
10 and the healthcare they received.

11           422. Had MultiCare disclosed that its data privacy was inadequate or that it did not  
12 adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor  
13 any reasonable person would have purchased healthcare from MultiCare and/or its affiliated  
14 healthcare providers.

15           423. As a direct and proximate result of the disclosure of Plaintiff's and Class  
16 Members' Private Information to Meta and Google, Plaintiff and Class Members have been  
17 harmed and have suffered, and will continue to suffer, actual damages and injuries, including  
18 without limitation the release, disclosure, and publication of their Private Information, the loss  
19 of control and diminution in value of their Private Information, the imminent risk of suffering  
20 additional damages in the future, disruption of their medical care and treatment, out-of-pocket  
21 expenses, and the loss of the benefit of the bargain they had struck with MultiCare.

22           424. Plaintiff and Class Members are entitled to compensatory and consequential  
23 damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private  
24 Information to Meta and Google.

**COUNT THREE****Breach of Implied Duty of Good Faith and Fair Dealing  
(*On behalf of Plaintiff & the Nationwide Class*)**

425. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

426. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with MultiCare for the provision of medical and health care services.

427. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with MultiCare when Plaintiff first received medical care from MultiCare.

428. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with MultiCare include MultiCare's implied duty of good faith and fair dealing, particularly due to MultiCare's special relationship with Plaintiff as his healthcare provider.

429. Under these express contracts, MultiCare and/or their affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiff and Class Members. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

430. In service of their implied duty of good faith and fair dealing when executing the contract, MultiCare were bound to not voluntarily divulge Plaintiff's and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

431. The express contracts for the provision of medical services are formed and embodied in multiple documents.

432. As evidence of MultiCare's knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiff's expectations of MultiCare to do the same, at all relevant times, MultiCare expressly

represented in its Privacy Notice, among other things: (i) that “We understand that information about you and your medical and behavioral health is personal. We are committed to protecting health information about you and are required under federal and state law to take steps to protect this information.”<sup>97</sup>; and (ii) that “MultiCare has security measures in place to prevent the loss, misuse or alteration of information under our control. MultiCare employs strict security measures to safeguard online financial transactions through the use of current industry encryption standards.”<sup>98</sup>

433. MultiCare’s express representations, including, but not limited to, express representations found in its Privacy Notice, evidence MultiCare’s knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required MultiCare to implement data security adequate to safeguard and protect the privacy of Plaintiff’s and Class Members’ Private Information.

434. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

435. Plaintiff and Class Members would not have entered into these contracts with MultiCare and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

436. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to MultiCare and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the

---

<sup>97</sup> <https://www.multicare.org/wp-content/uploads/2020/12/Notice-of-Privacy-Practices.pdf> (last visited June 18, 2024)

<sup>98</sup> <https://www.multicare.org/about/policies-notices/website-privacy-policy/> (last visited June 18, 2024)

1 provision of healthcare and medical services and, through MultiCare's implied duty of good  
2 faith and fair dealing, the protection of their Private Information.

3 437. Plaintiff and Class Members performed their obligations under the contract  
4 when they paid for their health care services and provided their Private Information.

5 438. MultiCare did not maintain the privacy of Plaintiff's and Class Members'  
6 Private Information as evidenced by MultiCare's sharing of that Private Information with  
7 Google and Meta through the Google and Meta Collection Tools on the Web Properties.

8 439. MultiCare breached its implied duty of good faith and fair dealing to protect the  
9 nonpublic Private Information MultiCare gathered when it disclosed that Private Information  
10 to Google and Meta through the Google and Meta Collection Tools on the Web Properties.

11 440. The mass and systematic disclosure of Plaintiff's and Class Members' Private  
12 Information to third parties, including Meta and Google, was a reasonably foreseeable  
13 consequence of MultiCare's actions in breach of its implied duty of good faith and fair  
14 dealing.

15 441. As a result of MultiCare's failure to fulfill the data privacy protections inherent  
16 in the special relationship with Plaintiff and the Class Members, and resulting breach of their  
17 implied duty of good faith and fair dealing, Plaintiff and Members of the Class did not receive  
18 the full benefit of the bargain, and instead received healthcare and other services that were of  
19 a diminished value to that described in the contracts.

20 442. Plaintiff and Class Members therefore were damaged in an amount at least  
21 equal to the difference in the value of the healthcare with data privacy protection they paid for  
22 and the healthcare they received.

23 443. Had MultiCare disclosed that its data privacy was inadequate or that they did  
24 not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members,  
25 nor any reasonable person would have purchased healthcare from MultiCare and/or its  
26 affiliated healthcare providers.



444. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with MultiCare.

445. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google.

**COUNT FOUR**  
**Breach of Implied Contract**  
*(On behalf of Plaintiff & the Nationwide Class)*

446. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

447. Plaintiff and Class Members allege they entered into valid and enforceable implied contracts or were third-party beneficiaries of valid and enforceable implied contracts, with MultiCare for the provision of medical and health care services.

448. Specifically, Plaintiff and Class Members entered into a valid and enforceable contract with MultiCare when Plaintiff first received medical care from MultiCare.

449. The valid and enforceable contracts to provide medical and health care services that Plaintiff and Class Members entered into with MultiCare include MultiCare's promise to protect nonpublic, Private Information given to MultiCare or that MultiCare gathers on its own from disclosure.

450. Under these contracts, MultiCare and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare;

and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

451. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these contracts.

452. The contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) MultiCare's Privacy Notice.

453. At all relevant times, MultiCare expressly represented in its Privacy Notice, among other things: (i) that "We understand that information about you and your medical and behavioral health is personal. We are committed to protecting health information about you and are required under federal and state law to take steps to protect this information."<sup>99</sup>; and (ii) that "MultiCare has security measures in place to prevent the loss, misuse or alteration of information under our control. MultiCare employs strict security measures to safeguard online financial transactions through the use of current industry encryption standards."<sup>100</sup>

454. MultiCare's express representations, including, but not limited to, express representations found in its Privacy Notice, formed and embodied an express contractual obligation requiring MultiCare to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

455. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful

<sup>99</sup> <https://www.multicare.org/wp-content/uploads/2020/12/Notice-of-Privacy-Practices.pdf> (last visited June 18, 2024).

<sup>100</sup> <https://www.multicare.org/about/policies-notices/website-privacy-policy/> (last visited June 18, 2024).

1 and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and  
2 Class Members would not have entered into these contracts with MultiCare and/or its  
3 affiliated healthcare providers as a direct or third-party beneficiary without an understanding  
4 that their Private Information would be safeguarded and protected.

5 456. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed  
6 to and did provide their Private Information to MultiCare and/or its affiliated healthcare  
7 providers, and paid for the provided healthcare in exchange for, amongst other things, both the  
8 provision of healthcare and medical services and the protection of their Private Information.

9 457. Plaintiff and Class Members performed their obligations under the contract  
10 when they paid for their health care services and provided their Private Information.

11 458. MultiCare materially breached its contractual obligation to protect the nonpublic  
12 Private Information MultiCare gathered when it disclosed that Private Information to Google  
13 and Meta through the Google and Meta Collection Tools on the Web Properties.

14 459. MultiCare materially breached the terms of these contracts, including, but not  
15 limited to, the terms stated in the relevant Privacy Notice. MultiCare did not maintain the  
16 privacy of Plaintiff's and Class Members' Private Information as evidenced by MultiCare's  
17 sharing of that Private Information with Google and Meta through the Google and Meta  
18 Collection Tools on the Web Properties.

19 460. The mass and systematic disclosure of Plaintiff's and Class Members' Private  
20 Information to third parties, including Meta and Google, was a reasonably foreseeable  
21 consequence of MultiCare's actions in breach of these contracts.

22 461. As a result of MultiCare's failure to fulfill the data privacy protections promised  
23 in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the  
24 bargain, and instead received healthcare and other services that were of a diminished value to  
25 that described in the contracts. Plaintiff and Class Members therefore were damaged in an  
26  
27

1 amount at least equal to the difference in the value of the healthcare with data privacy  
2 protection they paid for and the healthcare they received.

3 462. Had MultiCare disclosed that its data privacy was inadequate or that it did not  
4 adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor  
5 any reasonable person would have purchased healthcare from MultiCare and/or its affiliated  
6 healthcare providers.

7 463. As a direct and proximate result of the disclosure of Plaintiff's and Class  
8 Members' Private Information to Meta and Google, Plaintiff and Class Members have been  
9 harmed and have suffered, and will continue to suffer, actual damages and injuries, including  
10 without limitation the release, disclosure, and publication of their Private Information, the loss  
11 of control and diminution in value of their Private Information, the imminent risk of suffering  
12 additional damages in the future, disruption of their medical care and treatment, out-of-pocket  
13 expenses, and the loss of the benefit of the bargain they had struck with MultiCare.

14 464. Plaintiff and Class Members are entitled to compensatory and consequential  
15 damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private  
16 Information to Meta and Google.

## 17 **COUNT FIVE**

### 18 **Negligence**

#### 19 **(On behalf of Plaintiff & the Nationwide Class)**

20 465. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
21 forth herein.

22 466. MultiCare required Plaintiff and Class Members to submit non-public personal  
23 information in order to obtain healthcare services.

24 467. Upon accepting, storing, and controlling the Private Information of Plaintiff and  
25 the Class in their computer systems, MultiCare owed, and continues to owe, a duty to Plaintiff  
26 and the Class to exercise reasonable care to secure, safeguard and protect their highly  
27 sensitive Private Information from disclosure to third parties.

1           468. MultiCare’s duty of care to use reasonable measures to secure and safeguard  
2 Plaintiff’s and Class Members’ Private Information arose due, in part, to the special  
3 relationship that existed between MultiCare and its patients, which is recognized by statute,  
4 regulations, and the common law.

5           469. In addition, MultiCare had a duty under HIPAA privacy laws, which were  
6 enacted with the objective of protecting the confidentiality of clients’ healthcare information  
7 and set forth the conditions under which such information can be used, and to whom it can be  
8 disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations  
9 they work for, but to any entity that may have access to healthcare information about a patient  
10 that—if it were to fall into the wrong hands—could present a risk of harm to the patient’s  
11 finances or reputation.

12           470. MultiCare’s duty to use reasonable security measures under HIPAA required  
13 MultiCare to “reasonably protect” confidential data from “any intentional or unintentional use  
14 or disclosure” and to “have in place appropriate administrative, technical, and physical  
15 safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1).

16           471. Some or all of the healthcare, medical, and/or medical information at issue in  
17 this case constitutes “protected health information” within the meaning of HIPAA.

18           472. In addition, MultiCare had a duty to employ reasonable security measures under  
19 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . .  
20 practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the  
21 unfair practice of failing to use reasonable measures to protect confidential data.

22           473. MultiCare’s duty to use reasonable care in protecting confidential data arose  
23 also because MultiCare is bound by industry standards to protect confidential Private  
24 Information.

1           474. MultiCare breached this duty by failing to exercise reasonable care in  
2 safeguarding and protecting Plaintiff's and Class Members' Private Information from  
3 unauthorized disclosure.

4           475. It was reasonably foreseeable that MultiCare's failures to exercise reasonable  
5 care in safeguarding and protecting Plaintiff's and Class members' Private Information  
6 through its use of the Google and Meta Collection Tools and other tracking technologies  
7 would result in unauthorized third parties, such as Facebook and Google, gaining access to  
8 such Private Information for no lawful purpose.

9           476. MultiCare's own conduct also created a foreseeable risk of harm to Plaintiff and  
10 Class Members and their Private Information.

11           477. MultiCare's misconduct included the failure to (1) secure Plaintiff's and Class  
12 Members' Private Information; (2) comply with industry standard data security practices; (3)  
13 implement adequate website and event monitoring; (4) implement the systems, policies, and  
14 procedures necessary to prevent unauthorized disclosures resulting from the use of the Google  
15 and Meta Collection Tools and other tracking technologies; and (5) prevent unauthorized  
16 access to Plaintiff's and Class Members' Private Information by sharing that information with  
17 Meta, Google and other third parties. MultiCare's failures and breaches of these duties  
18 constituted negligence.

19           478. As a direct result of MultiCare's breaches of its duty of confidentiality and  
20 privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and  
21 the Class have suffered damages that include, without limitation, loss of the benefit of the  
22 bargain, increased infiltrations into their privacy through spam and targeted advertising they  
23 did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress,  
24 humiliation and loss of enjoyment of life.

479. MultiCare's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

480. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

481. MultiCare's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring MultiCare to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Meta, Google and other third parties without Plaintiff's and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

**COUNT SIX**  
**Breach of Fiduciary Duty**  
***(On Behalf of Plaintiff & the Nationwide Class)***

482. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

483. In light of the special physician-patient relationship between MultiCare and Plaintiff and Class Members, which was created for the purpose of MultiCare providing healthcare to Plaintiff and Class Members, MultiCare became guardian of Plaintiff's and Class Members' Private Information. MultiCare became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) MultiCare did and do store.



484. MultiCare has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients and former patients, in particular, to keep secure their Private Information.

485. MultiCare breached its fiduciary duty to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, including Meta and Google, and separately, by failing to notify Plaintiff and Class Members of this fact.

486. As a direct and proximate result of MultiCare's breaches of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

**COUNT SEVEN**  
**Unjust Enrichment**  
***(On behalf of Plaintiff & Nationwide Class)***

487. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

488. Plaintiff plead this claim in the alternative to their breach of contract claim.

489. Plaintiff and Class Members personally and directly conferred a benefit on MultiCare by paying MultiCare for health care services, which included MultiCare's obligations to protect Plaintiff's and Class Members' Private Information. MultiCare was aware of Plaintiff's privacy expectations, and in fact, promised to maintain Plaintiff's Private Information confidential and not to disclose to third parties. MultiCare received payments for medical services from Plaintiff and Class Members.

490. Plaintiff and Class Members also conferred a benefit on MultiCare in the form of valuable sensitive medical information that MultiCare collected from Plaintiff and Class Members under the guise of keeping this information private.

1           491. MultiCare collected, used, and disclosed this information for its own gain,  
2 including for advertisement, market research, sale, or trade for valuable benefits from  
3 Facebook, Google and other third parties.

4           492. MultiCare had knowledge that Plaintiff and Class Members had conferred this  
5 benefit on MultiCare by interacting with the Web Properties, and MultiCare intentionally  
6 installed the Google and Meta Collection Tools on the Web Properties to capture and  
7 monetize this benefit conferred by Plaintiff and Class Members.

8           493. Plaintiff and Class Members would not have used MultiCare's Web Properties  
9 had they known that MultiCare would collect, use, and disclose this information to Facebook,  
10 Google, and other third parties.

11           494. The services that Plaintiff and Class Members ultimately received in exchange  
12 for the monies paid to MultiCare were worth quantifiably less than the services that MultiCare  
13 promised to provide, which included MultiCare's promise that any patient communications  
14 with MultiCare would be treated as confidential and would never be disclosed to third parties  
15 for marketing purposes without the express consent of patients.

16           495. The medical services that MultiCare offers are available from many other health  
17 care systems that do protect the confidentiality of patient communications. Had MultiCare  
18 disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members'  
19 Private Health Information without consent, neither Plaintiff, the Class Members, nor any  
20 reasonable person would have purchased healthcare from MultiCare and/or its affiliated  
21 healthcare providers.

22           496. By virtue of the unlawful, unfair and deceptive conduct alleged herein,  
23 MultiCare knowingly realized hundreds of millions of dollars in revenue from the use of the  
24 Private Information of Plaintiff and Classes Members by way of targeted advertising related to  
25 Users' respective medical conditions and treatments sought.  
26  
27

497. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon MultiCare by Plaintiff and Class Members.

498. As a result of MultiCare's conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

499. It would be inequitable and unjust to permit MultiCare to retain the enormous economic benefits (financial and otherwise) it obtained from and/or at the expense of Plaintiff and Class Members.

500. MultiCare will be unjustly enriched if it is permitted to retain the economic benefits conferred upon it by Plaintiff and Class Members through MultiCare's obtaining the Private Information and the value thereof, and financially benefitting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiff and Class Members.

501. Plaintiff and Class Members are therefore entitled to recover the amounts realized by MultiCare at the expense of Plaintiff and Class Members.

502. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of MultiCare's ill-gotten gains, and/or other sums as may be just and equitable.

**COUNT EIGHT**  
**Invasion of Privacy**  
*(On Behalf of Plaintiff & the Nationwide Class)*

503. Plaintiff Darryl Small repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

1           504. The Private Information of Plaintiff and Class Members consists of private and  
2 confidential facts and information that was never intended to be shared beyond private  
3 communications.

4           505. Plaintiff and Class Members had a legitimate expectation of privacy regarding  
5 their Private Information and were accordingly entitled to the protection of this information  
6 against disclosure to unauthorized third parties.

7           506. Defendant owed a duty to Plaintiff and Class Members to keep their Private  
8 Information confidential.

9           507. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private  
10 Information to Facebook or Google, a third-party social media and marketing giants, is highly  
11 offensive to a reasonable person.

12           508. Defendant's willful and intentional disclosure of Plaintiff's and Class Members'  
13 Private Information constitutes an intentional interference with Plaintiff's and the Class  
14 Members' interest in solitude or seclusion, either as to their person or as to their private affairs  
15 or concerns, of a kind that would be highly offensive to a reasonable person.

16           509. Defendant's conduct constitutes an intentional physical or sensory intrusion on  
17 Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's and  
18 Google's simultaneous eavesdropping and wiretapping of confidential communications.

19           510. Defendant failed to protect Plaintiff's and Class Members' Private Information  
20 and acted knowingly when it installed the Meta and Google Collection Tools onto its Website  
21 because the purpose of the tools is to track and disseminate individual's communications with  
22 the Website for the purpose of marketing and advertising.

23           511. Because Defendant intentionally and willfully incorporated the Meta and Google  
24 Collection Tools into its Website and encouraged patients to use that Website for healthcare  
25 purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and  
26 Class Members.

512. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

513. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

514. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook and Google and the wrongful disclosure of the information cannot be undone.

515. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook and Google who on information and belief continues to possess and utilize that information.

516. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

## COUNT NINE

**Violation of the Washington Consumer Protection Act**  
**Wash. Rev. Code Ann. §§ 19.86.020, *et seq.***  
*(On Behalf of Plaintiff & the Washington Subclass)*

517. Plaintiff Darryl Small repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

518. MultiCare is a “person,” as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1           519. MultiCare advertised, offered, or sold goods or services in Washington and  
2 engaged in trade or commerce directly or indirectly affecting the people of Washington, as  
3 defined by Wash. Rev. Code Ann. § 19.86.010 (2).

4           520. MultiCare engaged in unfair or deceptive acts or practices in the conduct of  
5 trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

- 6           a.       Failing to secure and protect Plaintiff's and Washington Subclass  
7                   Members' Private Information in a confidential manner;
- 8           b.       Failing to inform Plaintiff and Washington Subclass Members of  
9                   Defendant's use of the Meta Pixel, Conversions API, Google Analytics,  
10                  and other tracking tools;
- 11          c.       Failing to inform Plaintiff and Washington Subclass Members of the  
12                  extent of Defendant's data harvesting, tracking, and disclosure practices;
- 13          d.       Failing to comply with common law and statutory duties pertaining to  
14                  the security and privacy of Plaintiff and Washington Subclass members'  
15                  Private Information, including duties imposed by the FTC Act, 15  
16                  U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§  
17                  6501-6505, which was a direct and proximate cause of the unauthorized  
18                  disclosure of their Private Information;
- 19          e.       Misrepresenting that it would protect the privacy and confidentiality of  
20                  Plaintiff and Washington Subclass members' Private Information,  
21                  including by implementing and maintaining reasonable security  
22                  measures;
- 23          f.       Misrepresenting that it would comply with common law and statutory  
24                  duties pertaining to the security and privacy of Plaintiff and Washington  
25                  Subclass members' Private Information, including duties imposed by the  
26  
27

1 FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15  
 2 U.S.C. §§ 6501-6505;

3 g. Misrepresenting that certain sensitive Private Information would not be  
 4 disclosed to third parties;

5 h. Omitting, suppressing, and concealing the material fact that it did not  
 6 reasonably or adequately secure Plaintiff and Washington Subclass  
 7 Members' Private Information and

8 i. Omitting, suppressing, and concealing the material fact that it did not  
 9 comply with common law and statutory duties pertaining to the security  
 10 and privacy of Plaintiff and Washington Subclass members' Private  
 11 Information, including duties imposed by the FTC Act, 15 U.S.C. § 45,  
 12 HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

13 521. Defendant's representations and omissions were material because they were  
 14 likely to deceive reasonable consumers about the adequacy of Defendant's ability and  
 15 intentions to protect the confidential and sensitive Private Information of Plaintiff and  
 16 Washington Subclass Members communicated for the purpose of medical treatment.

17 522. Defendant's representations and omissions were material because they were  
 18 likely to deceive reasonable consumers, including Plaintiffs and the Washington Subclass  
 19 Members, that their Private Information would be held in a secure and confidential manner,  
 20 rather than deliberately disclosed to third parties.

21 523. MultiCare acted intentionally, knowingly, and maliciously to violate  
 22 Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington  
 23 Subclass Members' rights.

24 524. Defendant's conduct is injurious to the public interest because it violates Wash.  
 25 Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration  
 26 of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, et  
 27



seq.. Alternatively, Defendant's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons.

525. Further, MultiCare's conduct affected the public interest including the thousands of Washington Residents impacted by its use of the Meta Pixel, Conversions API, Google Analytics and other tracking tools.

526. As a direct and proximate result of MultiCare's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including the damage to their privacy and property interests in their Private Information.

527. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties and attorneys' fees and costs.

### **IX. PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and all those similarly situated, respectfully requests this Honorable Court to grant the following relief:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

1. Preventing MultiCare from sharing Plaintiff's and Class Members' Private Information among other third parties;
2. Requiring MultiCare to alert and/or otherwise notify all Users of the Web Properties of what information is being collected, used, and shared;

3. Requiring MultiCare to provide clear information regarding its practices concerning data collection from the Users/patients of MultiCare's Web Properties, as well as uses of such data;
4. Requiring MultiCare to establish protocols intended to remove all personal information which has been leaked to Facebook, Google and/or other third parties, and request Facebook/Google/third parties to remove such information;
5. Requiring MultiCare to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with MultiCare's Web Properties;
6. Mandating the proper notice be sent to all affected individuals, and posted publicly;
7. Requiring MultiCare to delete, destroy, and purge the Private Information of Users unless MultiCare can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;
8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against MultiCare to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring MultiCare to cooperate and financially support civil and/or criminal asset recovery efforts;

1 E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including  
2 pursuant to statutory rates of interest set under State law);

3 F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs  
4 of suit incurred by their attorneys;

5 G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as  
6 they are allowed by applicable laws; and

7 H. Any and all other such relief as the Court may deem just and proper under the  
8 circumstances.

9 **X. JURY TRIAL DEMANDED**

10 Plaintiff demands a jury trial on all triable issues.

11 Dated: July 10, 2024

Respectfully submitted,

12 By: /s/ Samuel J. Strauss, WSBA #46971

13 Samuel J. Strauss, WSBA #46971

14 Email: sam@straussborrelli.com

STRAUSS BORRELLI PLLC

One Magnificent Mile

15 980 N Michigan Avenue, Suite 1610

16 Chicago, Illinois 60611

17 Telephone: (872) 263-1100

Facsimile: (872) 263-1109

18 *Attorneys for Plaintiff and the Class*